****Vulnerability scans/ Vulnerability (such as Nessus) 9**

General terms associated with CVEs/vulnerabilities. 9

How to tell if a particular vulnerable Apache module is being used/loaded in SecureSyncs 10

Specific vulnerabilities 11

June 2020 ntp-4.2.8p15 NTP Release and Security Vulnerability Announcement 11

Sec 3661 (in 4.2.8p15, Memory leak with CMAC keys) (23 June 2020) 11

March 2020 ntp-4.2.8p14 NTP Release and Security Vulnerability Announcement 11

SEC 3610 (process_control() should bail earlier on short packets.) (~May 2020) 11

SEC 3592 (Denial of Service attack on Unauthenticated Client) (~May 2020) 11

March 2019 ntp-4.2.8p13 NTP Release and Security Vulnerability Announcement 12

CVE's/CWE's Potential Vulnerabilities (All network appliances) 16

All recently updated CVEs 16

Zero-day Vulnerabilities 16

Procedure to follow when a previously unreported vulnerability (with any of our products) has been reported to us. 16

****NTP Vulnerabilities / NTP Bugs 17**

Vulnerability Note VU#633847 (21 Nov 2016, several new denial of service CVEs fixed in NTP version 4.2.8p9) 17

Vulnerability Note (several new CVEs fixed in NTP versions 4.2.8p7 and 4.2.8p8 – with our version 5.4.5 update, Sept 2016) 17

NTP Bug 2246 19

CVE-2015-5146 (ntpd control message crash: Crafted NUL-byte in configuration directive) 23

CVE-2015-1799 (NTP Symmetric Key) 24

CVE-2015-1798 (NTP Symmetric Key) 24

CVE-2014-9296 24

CVE-2014-9295 (NTP Autokey) 24

CVE-2014-9294 25

CVE-2014-9293 25

CVE-2013-5211 (Monlist in NTPDC) 25

******Debian vulnerabilites (Model 1232 VelaSync OS) 28**

All other vulnerabilities (not associated with NTP or Debian) 30

CWE's: The Common Weakness Enumeration numbers (such as CWE#20, for example) 30

Apache Struts and Apache Tomcat (AKA "Tomcat Server") 31

"SSH Weak MACs/SSH Weak Message Authentication Code Algorithms" 31

CGI Generic SQL Injection (CWE#20, CWE#77, CWE#751, CWE#722, CWE#91, CWE#203, CWE#643, CWE#713, CWE#801, CWE#89, CWE#928, CWE#929") 32

Possible Scan interference ("QID 42432 - Possible Scan Interference") 35

Web Server Vendor / Version Disclosure....35

“Missing HttpOnly Flag From Cookie” / “Missing Secure Flag From SSL Cookie”....35

“Apache 2.4.x < 2.4.54 Multiple Vulnerabilities” (~Sept 2022)....37

CVE-2023-27522 (Apache)....39

CVE-2023-25690 (Apache)....40

CVE-2023-0401 (PKCS7 for OpenSSL/HTTPS Certificates)....41

CVE-2023-0217 (PKCS7 for OpenSSL/HTTPS Certificates)....42

CVE-2023-0286 (x.509 HTTPS certificates)....42

CVE-2023-0217 (PKCS7 for OpenSSL/HTTPS Certificates)....43

CVE-2023-0216 (PKCS7 for OpenSSL/HTTPS Certificates)....43

CVE-2023-0215 (OpenSSL)....44

CVE-2022-42889 (Apache)....45

CVE-2022-37454 (SHA-3)....46

QID 150640 (CVE-2022-37436 and CVE-2022-36760)....46

CVE-2022-31813 (Apache)....49

CVE-2022-31630 (PHP)....49

CVE-2022-31629 (PHP)....51

CVE-2022-31628 (PHP)....52

CVE-2022-31626 (PHP with MySQL)....53

CVE-2022-31625 (PHP)....53

CVE-2022-30556 (Apache)....55

CVE-2022-30522 (Apache)....55

CVE-2022-29404 (Apache)....56

CVE-2022-28614 (Apache)....57

CVE-2022-28615 (Apache)....58

CVE-2022-28330 (Apache in Windows)....58

CVE-2022-26377 (Apache)....59

CVE-2022-23812 (package node-ipc)....60

CVE-2022-23943 (Apache)....60

CVE-2022-22963 and CVE-2022-22965: Spring Framework vulnerability and Spring4Shell exploit (Spring Framework)....61

CVE-2022-22721 (Apache)....62

CVE-2022-22720 (Apache)....62

CVE-2022-22719 (Apache)....63

CVE-2022-4450 (OpenSSL/HTTPS Certificates)....64

CVE-2022-4304 () 65

CVE-2022-4203 (x.509 HTTPS certificate) 65

CVE-2022-3786 (OpenSSL vulnerability for TLS HTTPS certificates) 66

CVE-2022-3602 (OpenSSL vulnerability for TLS HTTPS certificates) 67

CVE-2022-0847 (Dirty Pipe vulnerability in linux kernels) 67

CVE-2021-44790 (Apache) 68

CVE-2021-44224 (Apache) 69

CVE-2021-39275 (Apache) 70

CVE-2021-40438 (Apache Mod_Proxy)........ 71

CVE-2021-36160 (Apache) 71

CVE-2021-34798 (Apache) 73

CVE-2021-30641 (Apache) 73

CVE-2021-27108 (PHP)........ 75

CVE-2021-27105 (PHP)........ 76

CVE-2021-27104 (PHP when using Firebird PDO driver extension)........ 77

CVE-2021-27103 (PHP with Accellion) 77

CVE-2021-26691 (Apache) 78

CVE-2021-26690 (Apache) 79

CVE-2021-21704 and CVE-2021-21705 (PHP v7.4.6) 80

CVE-2021-21708 (PHP “php_filter_float function”)........ 81

CVE-2021-21707 (PHP)........ 82

CVE-2021-21703 (PHP)........ 83

CVE-2021-21702 (PHP)........ 84

CVE-2021-4034 (Polkit linux vulnerability) 84

CVE-2021-3156 CVE-2021-23239 CVE-2021-23240 (Sudo vulnerabilities) 85

CVE-2020-11896/CVE-2020-11897/CVE-2020-11898/CVE-2020-11899) “Ripple20” 86

CVE-2020-13938 (Apache) 87

CVE-2020-11993 (Apache browser vulnerability) 88

CVE-2020-11984 (Apache mod_proxy) 88

CVE-2020-9490 (Apache browser vulnerability) 89

CVE-2020-7068 (PHP - Use-After-Free Issue) 90

CVE-2020-1967 (OpenSSL vulnerability) 90

CVE-2019-18218 (file -- security update) 91

CVE-2019-17567 (Apache) 91

CVE-2019-15296 (Debian linux, linux-4.9 -- security update) 92

CVE-2019-15292 (Debian linux, linux-4.9 -- security update) 92

CVE-2019-15166 (tcpdump -- security update) 93

CVE-2019-16227 (tcpdump -- security update) 93

CVE-2019-14287 (sudo -- security update) 93

CVE-2019-12735 (neovim, vim -- security update) 93

CVE-2019-11815 (Debian linux, linux-4.9 -- security update) 94

CVE-2019-11043 (php5, php7.0, php7.3 -- security update) 94

CVE-2019-10126 (linux, linux-4.9 -- security update) 95

CVE-2019-10098 / CVE-2019-10097 / CVE-2019-10092 / CVE-2019-10082 / CVE-2019-10081 95

CVE-2019-9517 95

CVE 2019-6111, CVE 2019-6110, CVE 2019-6109 (OpenSSH) 96

CVE-2019-1563 (OpenSSL vulnerability) 96

CVE-2019-1559 (OpenSSL vulnerability) 97

CVE-2019-1551 (OpenSSL vulnerability) 98

CVE-2019-1547 (OpenSSL vulnerability) 98

CVE-2019-0190 100

CVE-2018-17199 / CVE-2018-17190 / CVE-2018-17189 101

CVE-2018-17082 (PHP vulnerability) 101

CVE-2018-16451 (tcpdump -- security update) 103

CVE-2018-16230 (tcpdump -- security update) 103

CVE-2018-16229 (tcpdump -- security update) 103

CVE-2018-16227 (tcpdump -- security update) 104

CVE-2018-15473 (OpenSSH vulnerability) 104

CVE-2018-10933 (libssh exploit) 108

CVE-2018-14882 (Debian: CVE-2018-14882: tcpdump -- security update) 108

CVE-2018-14470 (: tcpdump -- security update) 108

CVE-2018-14464 (tcpdump -- security update) 109

CVE-2018-14461 tcpdump -- security update) 109

CVE-2018-14633 (Debian linux, linux-4.9 -- security update) 109

CVE-2018-10933 (libssh exploit) 110

CVE-2018-10549 / CVE-2018-10548 / CVE-2018-10546 / CVE-2018-10545 (PHP vulnerability) 110

CVE-2018-10103 (tcpdump -- security update) 111

CVE-2018-5968 (Jackson DataBind - A deserialization of untrusted data vulnerability") 111

CVE-2018-5732 (DHCP) 111

CVE-2018-5407: (Port Smash / Hyper-Threading) 112

CVE-2018-5381, CVE-2018-5380, CVE-2018-5379, CVE-2018-5378 (Quagga BGP for NTP over Anycast mode) 113

CVE-2018-0732 (OpenSSL vulnerability) 115

CVE-2018-5407 (OpenSSL vulnerability) 115

CVE-2017-16650 (Linux Kernel ‘drivers/net/usb/qmi_wwan.c’ Local Denial of service) 116

CVE-2017-10911 Update for linux kernel Xen Block interface information disclosure vulnerability 117

CVE-2017-1000364, CVE-2017-1000365, CVE-2017-1000370, CVE-2017-1000371 and CVE-2017-1000379 (Stack Clash) 118

CVE-2017-12617 (tomcat: Remote Code Execution bypass for CVE-2017-12615) 118

CVE-2017-11108 CVE-2017- (11541-11544), CVE-2017-(12893-12902), CVE-2017-(12985-13055), CVE-2017- (13687-13690), CVE-2017-13725 (tcpdump?) 118

CVE-2017-9805 (Apache Struts 2 REST plugin Remote Code Execution) 119

CVE-2017-9798 (OptionsBleed) 120

CVE-2017-9445 (associated with systemd) 120

CVE-2017-7679, CVE-2017-7668, CVE-2017-3169, CVE-2017-3167 (mod_mime) 121

CVE-2017-7494 Samba: loading shared modules from any path in the system leading to RCD 122

CVE-2017-3735, CVE-2017-3736, CVE-2017-3737 and CVE-2017-3738 123

CVE-2017-3732 (OpenSSL vulnerability) 124

CVE-2017-3731 (OpenSSL vulnerability) 124

CVE-2017-3730 (OpenSSL vulnerability) 124

CVE-2016-10150 (Debian linux -- security update) 125

CVE-2016-8743 / CVE-2016-8740 125

CVE-2016-7055 (OpenSSL vulnerability) 125

CVE-2017-5638 “Apache Struts2 Content-Type Input Validation Code Execution Vulnerability.” 126

CVE-2016-5387 126

CVE-2016-5195 “Kernel Local Privilege Escalation” (AKA “Dirty COW”) 127

CVE-2016-4979 129

CVE-2016-4049 “buffer overflow in bgpd” (related to Quagga) 129

CVE-2016-3115 129

CVE-2016-2342 “buffer overflow in bgpd” (related to Quagga) 129

CVE-2016-2183/CVE-2016-6329 (DES and Triple DES ciphers, Birthday attack, Sweet 32/Sweet32 attack) 130

CVE-2016-2161/CVE-1546 131

CVE-2016-0736 131

CVE-2015-2808: “ssl rc4 cipher suites supported vulnerability” 132

**RC4 (also known as ARC4 or ARCFour) 132

To mitigate potential vulnerabilities associated with RC4 133

CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2109, CVE-2016-2176, CVE-2016-0702, CVE-2016-0705, CVE-2016-0797, CVE-2016-0798, CVE-2016-0799, CVE-2016-0800 (all associated with OpenSSL version) 134

CVE-2015-7547 (glibc security and two bug fix update) 135

A) Potential Security Vulnerability 135

B) This update also fixes the following two bugs: 135

CVE-2015-5621 (net-snmpd) 135

CVE-2015-5600 (openssh – "MaxAuthTries bypass") 136

CVE-2015-5352 (OpenSSH Client Rejected `HostCertificate` Handling Vulnerability) 136

CVE-NONE-0791 (OpenSSH `PermitRootLogin` Security Bypass Vulnerability) 137

CVE-2015-4000 ("TLS Diffie-Hellman Key Exchange Logjam vulnerability" for SSL/TLS) 138

CVE-2015-3183 139

CVE-2015-1793 140

CVE-2015-1792 140

CVE-2015-1791 141

CVE-2015-1790 141

CVE-2015-1789 141

CVE-2015-1788 142

CVE-2014-3581 / CVE-2014-3583 142

CVE-2014-2830 (Stack-based buffer overflow in cifskey.c or cifscreds.c) 142

CVE-2014-0076 (Montgomery ladder in OpenSSL) 143

Multiple CVEs associated with versions of PHP and other libraries 143

CVE-2012-6708 (jQuery vulnerability) 144

CVE-2012-2141 Net-SNMP Denial of Service (Zero-Day) 144

CVE-2004-2761 SSL Certificate Signed using Weak Hashing Algorithm 145

"SSL Certificate - Signature Verification Failed Vulnerability" ("port 443/tcp over SSL") 145

"SSL Certificate signed with an unknown Certificate Authority" 145

PCI DSS compliance (Payment Card Industry) 146

FTP being enabled 146

Telnet being enabled 147

OpenSSH 148

A) "OpenSSH <=6.6 SFTP misconfiguration exploit for 64bit Linux – Remote" 148

B) SSH Local Access Not Available 148

Web browser (HTTP/HTTPS) 148

A) "Web Resource /.cgi-bin/loigin_adv.tcl Detected" 148

B) Directly related to HTTP being enabled 148

C) Web Server Allows Password Auto-Completion (PCI-DSS variant) 148

CVE-1999-0524 “ICMP TimeStamp Request” 151

"TCP Sequence Number Approximation Based Denial of Service” (NISCC Vulnerability Advisory 236929) 152

CVE-2004-0790, CVE-2004-0791, and CVE-2004-1060 CVE-2005-0065, CVE-2005-0066, CVE-2005-0067, and CVE-2005-0068 . 152

Related CVE’s 152

CVE-2004-0230 (TCP) 153

CVE-2004-0790 (TCP) 153

CVE-2004-1653 (“OpenSSH >= 2.3.0 AllowTcpForwarding Port Bouncing”) 153

CVE 2004-2004 153

CVE 2004-2761 (MD5 Message-Digest Algorithm is not collision resistant) 154

CVE-2007-2243 and CVE-2007-2768 “OpenSSH S/KEY Authentication Account Enumeration” and 155

“OPIE w/ OpenSSH Account Enumeration” 155

CVE-2007-2243 and CVE-2008-1483 OpenSSH 156

CVE-2008-1483 (OpenSSH X11 Forwarding Information Disclosure Vulnerability) 156

CVE-2008-3259 (OpenSSH "X11UseLocalhost" X11 Forwarding Session Hijacking Vulnerability) 157

CVE-2008-5161 (OpenSSH CBC Mode vulnerability) 157

CVE-2008-7270 (SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled) 159

CVE-2010-4180 160

CVE-2010-5107 161

CVE-2011-3192 (Denial of Service attack) 162

CVE-2011-3389 httpd: cookie exposure due to error responses (AKA “Beast” Attack) 163

SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability 163

CVE-2012-0053 (Apache HTTP Server httpOnly information disclosure) 166

Prevent Cross Site Request Forgery (CSRF) attacks 168

CVE-2012-1823 (PHP 'php-cgi' Information Disclosure Vulnerability) 169

CVE-2012-4929 / CVE-2012-4930 TLS CRIME Vulnerabilities (TLS version 1.2) 171

CVE-2012-4930 171

CVE-2013-0169 171

CVE-2013-2566 (SSL/TLS use of weak RC4 cipher) 172

CVE 2014-0195 (dtls1_reassemble_fragment function) 173

CVE 2014-0198 (do_ssl3_write function in s3_pkt.c) 174

CVE 2014-0221 (do_ssl3_write function in s3_pkt.c) 174

CVE-2014-0224: 'ChangeCipherSpec' MiTM Vulnerability/OpenSSL Server-Side ChangeCipherSpec Injection Scanner 175

CVE 2014-3470 (do_ssl3_write function in s3_pkt.c) 175

CVE-2014-3505, CVE-2014-3506, CVE-2014-3507, CVE-2014-3508, CVE-2014-3509, CVE-2014-3510, CVE-2014-3511, CVE-2014-3512, CVE-2014-5139........ 176

CVE-2014-3566 (Poodle) 176

CVE-2014-3569 (Null pointer Derefence) 177

CVE-2014-3570 (BN_sqr implementation)........ 177

CVE-2014-3571 (Null pointer Derefence) 178

CVE-2014-3572 (ssl3_get_key_exchange) 178

CVE-2014-8176 (dtls1_clear_queues function) 179

CVE-2014-8275 179

CVE-2014-8730 (a variant of Poodle)........ 180

ICS-CERT Advisory (ICSA-14-353-01) CVE-2014-9296, CVE-2014-9295 CVE-2014-9294, CVE-2014-9293 180

CVE-2015-0204 and CVE-2015-1067 (“Freak attack”) (ssl3_get_key_exchange function)........ 180

CVE-2015-0205 (ssl3_get_cert_verify function) Man in the Middle Security Bypass Vulnerability 181

CVE-2015-0206 (Memory leak in the dtls1_buffer_record function) 181

CVE-2015-0235 (AKA “Ghost”) glibc gethostbyname buffer overflow 182

CVE-2015-1637 (also associated with “Freak Attack) 182

CVE-2015-2808 (BAR Mitzvah attack associated with the RC4 cipher) 183

CVE-2015-4000 TLS Diffie-Hellman Key Exchange Logjam Vulnerability (RC4 cipher) 184

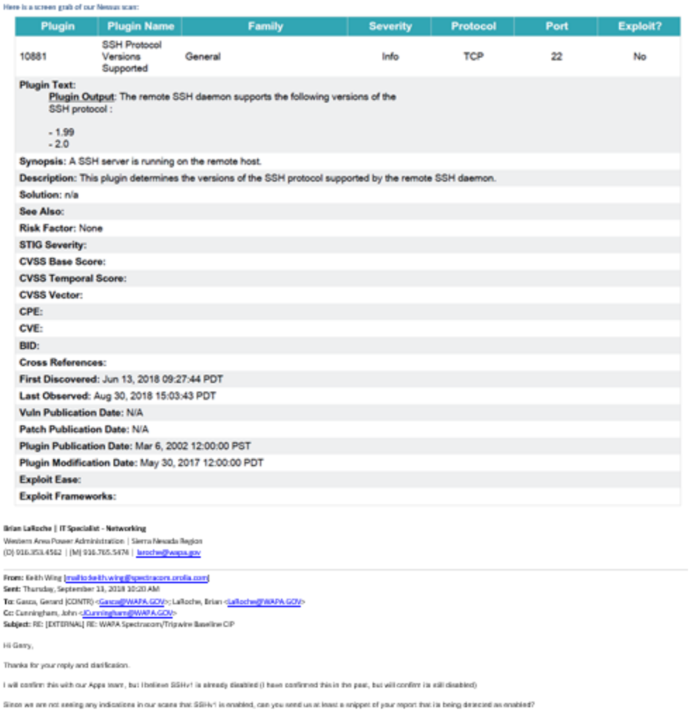
CVE-2015-9251 (jQuery vulnerability) 185

**Vulnerability scans/ Vulnerability (such as Nessus)

A) Tenerable Nessus ("Nessus")

- Is compatible with our products, such as SecureSyncs/NetClocks

B) Example screengrab from a Nessus Scan performed on SecureSync



Here is a screen grab of our Nessus scan:

Plugin	Plugin Name	Family	Severity	Protocol	Port	Exploit?
10881	SSH Protocol Versions Supported	General	Info	TCP	22	No

Plugin Text:
Plugin Output: The remote SSH daemon supports the following versions of the SSH protocol :

- 1.99
- 2.0

Synopsis: A SSH server is running on the remote host.

Description: This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution: n/a

See Also:

Risk Factor: None

STIG Severity:

CVSS Base Score:

CVSS Temporal Score:

CVSS Vector:

CPE:

CVE:

BID:

Cross References:

First Discovered: Jun 13, 2018 09:27:44 PDT

Last Observed: Aug 30, 2018 15:03:43 PDT

Vuln Publication Date: N/A

Patch Publication Date: N/A

Plugin Publication Date: Mar 6, 2002 12:00:00 PST

Plugin Modification Date: May 30, 2017 12:00:00 PDT

Exploit Ease:

Exploit Frameworks:

Brian LaRoche | IT Specialist - Networking
Western Area Power Administration | Sierra Nevada Region
(O) 916.353.4562 | (M) 916.765.5474 | laroche@wapa.gov

From: Keith Wing [mailto:keith.wing@spectracom.orolia.com]
Sent: Thursday, September 13, 2018 10:20 AM
To: Garza, Gerard (CONTR) <Garza@WAPA.GOV>; LaRoche, Brian <LaRoche@WAPA.GOV>
Cc: Cunningham, John <JCunningham@WAPA.GOV>
Subject: RE: [EXTERNAL] RE: WAPA Spectracom/Tripwire Baseline CIP

Hi Garry,

Thanks for your reply and clarification.

I will confirm this with our Apps team, but I believe SSHv1 is already disabled (I have confirmed this in the past, but will confirm it is still disabled)

Since we are not seeing any indications in our scans that SSHv1 is enabled, can you send us at least a snippet of your report that is being detected as enabled?

General terms associated with CVEs/vulnerabilities.

- **LLMNR:**
  - Refer to Salesforce Case 301047
  - Refer to https://en.wikipedia.org/wiki/Link-Local_Multicast_Name_Resolution#:~:text=The%20Link%2DLocal%20Multicast%20Name,on%20the%20same%20local%20link.

    The Link-Local Multicast Name Resolution (LLMNR) is a protocol based on the Domain Name System (DNS) packet format that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link.

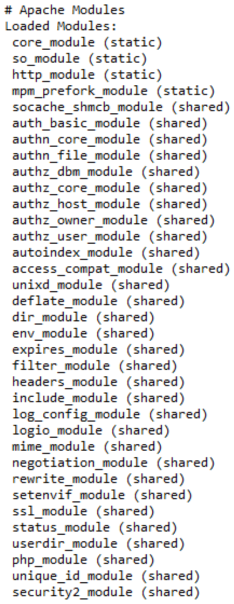
How to tell if a particular vulnerable Apache module is being used/loaded in SecureSyncs

Similar to PHP, how we specifically install Apache in the SecureSyncs can determine whether or not the device is susceptible to potential Apache CVEs.

Starting in update version 1.7.0, Engineering is now listing in the "**System_Component_Versions_2400_x.x.x.txt**" document (included in the Arena release documentation) all Apache modules in use. If a customer asks if the 2400 SecureSync is susceptible to an Apache CVE, just look at this document to see if an affected module is listed here (no longer need to escalate to apps to see if we use a particular module).

Note this same text doc has also provided for each release all the various versions for the CF cards, based on the main version of the SecureSync (this info can also be helpful for cases).

Below is an excerpt from the v1.7.0 release, showing all Apache modules loaded in 1.7.0



```
# Apache Modules
Loaded Modules:
 core_module (static)
 so_module (static)
 http_module (static)
 mpm_prefork_module (static)
 socache_shmcb_module (shared)
 auth_basic_module (shared)
 authn_core_module (shared)
 authn_file_module (shared)
 authz_dbm_module (shared)
 authz_core_module (shared)
 authz_host_module (shared)
 authz_owner_module (shared)
 authz_user_module (shared)
 autoindex_module (shared)
 access_compat_module (shared)
 unixd_module (shared)
 deflate_module (shared)
 dir_module (shared)
 env_module (shared)
 expires_module (shared)
 filter_module (shared)
 headers_module (shared)
 include_module (shared)
 log_config_module (shared)
 logio_module (shared)
 mime_module (shared)
 negotiation_module (shared)
 rewrite_module (shared)
 setenvif_module (shared)
 ssl_module (shared)
 status_module (shared)
 userdir_module (shared)
 php_module (shared)
 unique_id_module (shared)
 security2_module (shared)
```

Specific vulnerabilities

Note: Except NTP vulnerabilities, all being listed at the beginning - the rest are listed in ascending CVE number order with "no CVE number known" listed first.

A) NTP-related bugs (Bug) and vulnerabilities (Sec) (descending order)

- Refer to bugs.ntp.org and https://support.ntp.org/bin/view/Main/SecurityNotice
- Refer to the following site for a list of all NTP vulnerabilities: http://www.cvedetails.com/vulnerability-list/vendor_id-2153/NTP.html

June 2020 ntp-4.2.8p15 NTP Release and Security Vulnerability Announcement

Sec 3661 (in 4.2.8p15, Memory leak with CMAC keys) (23 June 2020)

- Refer to sites such as: https://support.ntp.org/bin/view/Main/SecurityNotice#June_2020_ntp_4_2_8p15_NTP_Relea

Severity: medium

Summary: Systems that use a CMAC algorithm in ntp.keys will not release a bit of memory on each packet that uses a CMAC key, eventually causing ntpd to run out of memory and fail. The CMAC cleanup from https://bugs.ntp.org/3447, part of ntp-4.2.8p11 and ntp-4.3.97, introduced a bug whereby the CMAC data structure was no longer completely removed.

Products:

- **VersaSync/VersaPNT**
- **1232 VelaSync**
- **Legacy VelaSync: N/A (doesn't use NTP software)**
- **NetClock 9300 and 9200 series**:
  - At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0). Note there are no further software updates expected for these NTP servers
- **1200 SecureSync/9400s**
  - No version of our software is affected.
  - Refer to Salesforce Case 213704

My response

As also confirmed by our Apps Engineering team, no version of SecureSync software is affected by this very recently discovered potential NTP vulnerability.

This potential vulnerability applies only to one specific type algorithm that NTP allows to be used for symmetric key NTP authentication (an optional "secret" shared passphrase configured in both the NTP server and its clients to authenticate the NTP server).

The SecureSync allows for certain algorithms to be selected from (MD5 and SHA are the most commonly used algorithms) when creating Symmetric keys to be used with the NTP clients. But the SecureSync doesn't support or allow "CMAC" to be selected as the desired algorithm. So, no symmetric keys using the "CMAC algorithm" can be created in the SecureSync.

March 2020 ntp-4.2.8p14 NTP Release and Security Vulnerability Announcement

SEC 3610 (process_control() should bail earlier on short packets.) (~May 2020)

SEC 3592 (Denial of Service attack on Unauthenticated Client) (~May 2020)

- Refer to sites such as: http://support.ntp.org/bin/view/Main/NtpBug3592

Summary: The fix for https://bugs.ntp.org/3445 introduced a bug whereby a system that is running ntp-4.2.8p12 or p13 that only has one unauthenticated time source can be attacked in a way that causes the victim's next poll to its source to be delayed, for as long as the attack is maintained.

Mitigation:

- Use authentication with symmetric peers.
- Have enough sources of time.
- Upgrade to 4.2.8p14, or later, from the NTP Project Download Page or the NTP Public Services Project Download Page.
  - (expected to be added in v5.9.0, ~Sept 2020)

Products:

- **VersaSyn/VersaPNT**
- **1232 VelaSync**
- **Legacy VelaSync: N/A (doesn't use NTP software)**
- **1200 SecureSync/9400s**
  - **At least versions 5.8.9 and below are susceptable**
- **NetClock 9300 and 9200 series**:
  - At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0). Note there are no further software updates expected for these NTP servers

March 2019 ntp-4.2.8p13 NTP Release and Security Vulnerability Announcement

Bug 3656/CVE-2019-8936 (NTP through 4.2.8p12 has a NULL Pointer Dereference)

- **Refer to sites such as:** https://nvd.nist.gov/vuln/detail/CVE-2019-8936

Fix: update NTP beyond NTPv4.2.8p12

Products:

- VersaSync/VersaPNT N/A (doesn't use NTP software)
- 1232 VelaSync N/A (doesn't use NTP software)
- **Legacy VelaSync**: N/A (doesn't use NTP software)
- **1200 SecureSync/9400s**
  - **At least versions 5.8. and below are susceptible**
- NetClock 9300 and 9200 series**:**
  - At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0). Note there are no further software updates expected for these NTP servers

CVE-2018-12327 (affects 4.2.8p11= update to 4.2.8p12 or above)

Refer to: https://nvd.nist.gov/vuln/detail/CVE-2018-12327

Stack-based buffer overflow in ntpq and ntpdc of NTP version 4.2.8p11 allows an attacker to achieve code execution or escalate to higher privileges via a long string as the argument for an IPv4 or IPv6 command-line parameter. NOTE: It is unclear whether there are any common situations in which ntpq or ntpdc is used with a command line from an untrusted source.

Products:

- **Legacy VelaSync**: N/A (doesn't use NTP software)

- **1200 SecureSync/9400s**
  - **Fixed in version 5.8.2????? software update (suspect it will be fixed in 5.8.2 but not confirmed by Dave Sohn yet, as of 21 Aug 2018)**

NetClock 9300 and 9200 series:
- At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0). Note there are no further software updates expected for these NTP servers.

CVE-2018-7185, CVE-2018-7184, CVE-2018-7183, CVE-2018-7182

- Refer to: CVE-2018-7185: https://nvd.nist.gov/vuln/detail/CVE-2018-7185
- The protocol engine in ntp 4.2.6 before 4.2.8p11 allows remote attackers to cause a denial of service (disruption) by continually sending a packet with a zero-origin timestamp and source IP address of the "other side" of an interleaved association causing the victim ntpd to reset its association
- CVE-2018-7184 https://nvd.nist.gov/vuln/detail/CVE-2018-7184
- ntpd in ntp 4.2.8p4 before 4.2.8p11 drops bad packets before updating the "received" timestamp, which allows remote attackers to cause a denial of service (disruption) by sending a packet with a zero-origin timestamp causing the association to reset and setting the contents of the packet as the most recent timestamp. This issue is a result of an incomplete fix for CVE-2015-7704.
- CVE-2018-7183 https://nvd.nist.gov/vuln/detail/CVE-2018-7183

  Buffer overflow in the decodearr function in ntpq in ntp 4.2.8p6 through 4.2.8p10 allows remote attackers to execute arbitrary code by leveraging an ntpq query and sending a response with a crafted array.

- CVE-2018-7182 https://nvd.nist.gov/vuln/detail/CVE-2018-7182
- The ctl_getitem method in ntpd in ntp-4.2.8p6 before 4.2.8p11 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mode 6 packet with a ntpd instance from 4.2.8p6 through 4.2.8p10.

Products:

- **Legacy VelaSync: N/A (doesn't use NTP software)**
- **1200 SecureSync/9400s**
  - **Fixed in version 5.8.0 software update (May 2018)**
- **NetClock 9300 and 9200 series**:
  - At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0). Note there are no further software updates expected for these NTP servers.

Vulnerability Note VU#325339 March 2017 ntp-4.2.8p10 NTP Security Vulnerability Announcement

- Refer to http://support.ntp.org/bin/view/Main/SecurityNotice#Recent_Vulnerabilities

NTF's NTP Project is releasing ntp-4.2.8p10, which addresses:

- 6 MEDIUM severity vulnerabilities (1 is about the Windows PPSAPI DLL)
- 5 LOW severity vulnerabilities (2 are in the Windows Installer)
- 4 Informational-level vulnerabilities

  - 15 other non-security fixes and improvements

- ➢ **Refer to:** http://support.ntp.org/bin/view/Main/NtpBug3389

Products:

- ○ **Legacy VelaSync: N/A (doesn’t use NTP software)**
- ○ **1200 SecureSync/9400s**
  - ➢ **At least software versions 5.6.0 and below are potentially affected Per Paul Myers (23 Mar 17), Gentoo has not yet added 4.2.8p10 yet (not yet considered stable). We are planning on upgrading NTP in 4.7.0 expected to be released in about two months.**
- ○ **NetClock 9300 and 9200 series**:
  - ➢ At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0). Note there are no further software updates expected for these NTP servers.

Details
ntp-4.2.8p10 was released on 21 March 2017.

NTF's NTP Project is releasing ntp-4.2.8p10, which addresses:

- 6 MEDIUM severity vulnerabilities (1 is about the Windows PPSAPI DLL)
- 5 LOW severity vulnerabilities (2 are in the Windows Installer)
- 4 Informational-level vulnerabilities

- 15 other non-security fixes and improvements

All of the security issues in this release are listed in VU#633849

- Sec 3389 / CVE-2017-6464 / VU#325339: NTP-01-016 NTP: Denial of Service via Malformed Config (Pentest report 01.2017)
- Sec 3388 / CVE-2017-6462 / VU#325339: NTP-01-014 NTP: Buffer Overflow in DPTS Clock (Pentest report 01.2017)
- Sec 3387 / CVE-2017-6463 / VU#325339: NTP-01-012 NTP: Authenticated DoS via Malicious Config Option (Pentest report 01.2017)
- Sec 3386: NTP-01-011 NTP: ntpq_stripquotes() returns incorrect Value (Pentest report 01.2017)
- Sec 3385: NTP-01-010 NTP: ereallocarray()/eallocarray() underused (Pentest report 01.2017)
- Sec 3384 / CVE-2017-6455 / VU#325339: NTP-01-009 NTP: Windows: Privileged execution of User Library code
- Sec 3383 / CVE-2017-6452 / VU#325339: NTP-01-008 NTP: Windows Installer: Stack Buffer Overflow from Command Line
- Sec 3382 / CVE-2017-6459 / VU#325339: NTP-01-007 NTP: Windows Installer: Data Structure terminated insufficiently
- Sec 3381: NTP-01-006 NTP: Copious amounts of Unused Code (Pentest report 01.2017)
- Sec 3380: NTP-01-005 NTP: Off-by-one in Oncore GPS Receiver (Pentest report 01.2017)
- Sec 3379 / CVE-2017-6458 / VU#325339: NTP-01-004 NTP: Potential Overflows in ctl_put() functions (Pentest report 01.2017)
- Sec 3378 / CVE-2017-6451 / VU#325339: NTP-01-003 Improper use of snprintf() in mx4200_send() (Pentest report 01.2017)
- Sec 3377 / CVE-2017-6460 / VU#325339: NTP-01-002 Buffer Overflow in ntpq when fetching reslist (Pentest report 01.2017)
- Sec 3376: NTP-01-001 Makefile does not enforce Security Flags (Pentest report 01.2017)
- Sec 3361 / CVE-2016-9042 / VU#325339: 0rigin

CVE’s/CWE’s Potential Vulnerabilities (All network appliances)

All recently updated CVEs: https://www.tenable.com/cve/updated?page=2

Zero-day Vulnerabilities

- Refer to sites such as: https://www.techrepublic.com/article/what-is-a-zero-day-vulnerability/
- A zero-day vulnerability is a flaw in a piece of software that is unknown to the programmer(s) or vendor(s) responsible for the application(s). Because the vulnerability isn’t known, there is no patch available.
- In other words, the vulnerability has been discovered by someone who isn’t directly involved with a project**. The term zero day refers to the days between the time the vulnerability was discovered and the first attack against it. After a zero-day vulnerability has been made public, it is then referred to as an n-day vulnerability.**
- Most often, exploits against a zero-day vulnerability are a very rarely discovered right away. It can often take days or months before these flaws are found which is what makes these types of vulnerabilities so dangerous.

Procedure to follow when a previously unreported vulnerability (with any of our products) has been reported to us.

A) Ask the customer for the CVE number for the reported vulnerability, if their scanner reports it.

B) If not reported by their scanner, Google search the text of the report to obtain the CVE number.

C) Refer to the CVE number for details on the severity, recommended fixes, etc.

Recommended references for info on vulnerabilities and version upgrades that mitigate the vulnerability:

- **NIST:** http://web.nvd.nist.gov/view/vuln/search
- **CVE Details** http://www.cvedetails.com/cve/CVE-2012-0053/
- **MITRE**: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0053

Recommended general actions for scanner findings

- Upgrade the device to the latest version of software
- Make sure Telnet, HTTP and FTP are disabled in the list of Services.
- 1200 SecureSync/9400: disable the classic interface (disables issues with CGI)

Note: Ability to disable the Classic interface was added in software version 5.1.4

**NTP Vulnerabilities / NTP Bugs

Vulnerability Note VU#633847 (21 Nov 2016, several new denial of service CVEs fixed in NTP version 4.2.8p9)

- Refer to: http://www.security-database.com/detail.php?alert=VU633847 and http://nwtime.org/ntp428p9_release/
- NTP v4.2.8P9 was released 21 Nov, 2016

Note Update version 5.5.0 updated NTP to version 4.2.8p9.

CVEs addressed in ntp-4.2.8p9 update, per this note:

- **CVE-2016-9311** NULL Pointer Dereference
- **CVE-2016-9310** Uncontrolled Resource Consumption ('Resource Exhaustion')
- **CVE-2016-7427** Uncontrolled Resource Consumption ('Resource Exhaustion')
- **CVE-2016-7428** Uncontrolled Resource Consumption ('Resource Exhaustion')
- **CVE-2016-9312** Insufficient Resource Pool
- **CVE-2016-7434** Improper Input Validation
- **CVE-2016-7429** Multiple Binds to the Same Port
- **CVE-2016-7426** Insufficient Resource Pool
- **CVE-2016-7433** Incorrect Calculation

Products:

- **Legacy 1225 VelaSync: N/A (doesn't use NTP software)**

- **1200 SecureSync/9400s**
  - At least software versions 5.4.5 and below are potentially affected (Version 5.4.5 updated NTP to version 4.2.8p8 which didn't fix these). V5.5.0 updated NTP to 4.2.8p9, which fixes these NTP bugs.
- **NetClock 9300 and 9200 series**:
  - At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0). Note there are no further software updates expected for these NTP servers.

Vulnerability Note (several new CVEs fixed in NTP versions 4.2.8p7 and 4.2.8p8 – with our version 5.4.5 update, Sept 2016)

A) CVEs addressed in ntp-4.2.8p8:

- **CVE-2016-4957** / VU#321640: Crypto-NAK crash;
- **CVE-2016-4953 /** VU#321640: Bad authentication demobilizes ephemeral associations;
- **CVE-2016-4954** / VU#321640: Processing spoofed server packets;
- **CVE-2016-4955** / VU#321640: Autokey association reset;
- **CVE-2016-4956** / VU#321640: Broadcast interleave

A) CVEs addressed in ntp-4.2.8p7:

- **CVE-2016-1551**: Refclock impersonation vulnerability, AKA: refclock-peering;
- **CVE-2016-1549**: Sybil vulnerability: ephemeral association attack, AKA: ntp-sybil - MITIGATION ONLY;
- **CVE-2016-2516**: Duplicate IPs on unconfig directives will cause an assertion botch;
- **CVE-2016-2517:** Remote configuration trustedkey/requestkey values are not properly validated;
- **CVE-2016-2518**: Crafted addpeer with hmode > 7 causes array wraparound with MATCH_ASSOC;
- **CVE-2016-2519**: ctl_getitem() return value not always checked;
- **CVE-2016-1547**: Validate crypto-NAKs, AKA: nak-dos;
- **CVE-2016-1548**: Interleave-pivot - MITIGATION ONLY;
- **CVE-2015-7704**: KoD fix: peer associations were broken by the fix for NtpBug2901, AKA: Symmetric active/passive mode is broken;

- **CVE-2015-8138**: Zero Origin Timestamp Bypass, AKA: Additional KoD Checks;
- **CVE-2016-1550**: Improve NTP security against buffer comparison timing attacks, authdecrypt-timing, AKA: authdecrypt-timing

- Refer to SR5271 in SAP
- VU#321640 report was released 2 June 2016 (Refer to https://www.kb.cert.org/vuls/id/321640)
- **Impact**: Unauthenticated, remote attackers may be able to spoof or send specially crafted packets to create denial of service conditions.
- All five vulnerabilities affect NTP versions 4.2.8p7 and below (all are fixed in version 4.2.8p8)
- As of 7 June, 4.2.8p8 is not yet released/available in gentoo. 4.2.8p7 is still the current version.

Products:

- **Legacy VelaSync: N/A (doesn't use NTP software)**
- 1200 **SecureSync/9400s**
  - **At least software versions 5.4.1 and below are potentially affected (Version 5.4.0 updated NTP to version 4.2.8p6 which didn't fix these. But version 5.4.5 updated NTP to version 4.2.8p8 which does fix these).**
- **NetClock 9300 and 9200 series**:
  - At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0). Note there are no further software updates expected for these NTP servers.

Temporary Work-around: **Per Paul Myers (6 Jun 16) From the email I sent you last night I don't think customers are impacted UNLESS they enable external NTP query or use Autokey. If they do not do this they should not be impacted.**

Note what Harlen Stenn says
http://support.ntp.org/bin/view/Main/SoftwareDownloads#Weak_default_key_in_config_auth

Our NTP conf file does not allow query. Advise them to not enable it.

And the last CVE-2014-9296 requires use of CRYPTO keyword which I think is used by Autokey. SO Don't use Crypto and you don't have this issue.

Six new NTP vulnerabilities reported in April, 2016 (CVE-2016-1551, CVE-2016-1550, CVE-2016-1549, CVE-2016-1548, CVE-2016-1547)

- Refer to Mantis case 3269
- These six vulnerabilities have been fixed in NTP version 4.2.8p7
- Refer to http://www.theregister.co.uk/2016/04/28/time_for_a_patch_six_vulns_fixed_in_ntp_daemon/
- At least software versions 5.4.1 and below (version 5.4.0 updated NTP to version 4.2.8p6).

Products:

- **Legacy VelaSync: N/A (doesn't use NTP software)**
- **1200 SecureSync/9400s**
  - **At least software versions 5.4.1 and below (version 5.4.0 updated NTP to version 4.2.8p6).**
- **NetClock 9300 and 9200 series**:
  - At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0). Note there are no further software updates expected for these NTP servers.

(Info below is from the link above)

…the vulnerabilities, discovered during its ongoing ntpd evaluation, “allow attackers to craft UDP packets to either cause a denial of service condition or to prevent the correct time being set”, Cisco's Talos Security Intelligence and Research Group writes here.

CVE-2016-1551, an NTP refclock impersonation vulnerability, is less serious. The vuln means packet spoofing would let the attacker alter the target's time, if the packets originate from the 127.127.0.0/16 address range as trusted.

However, as the post notes, the 127.127.0.0/8 range should be filtered out by operating systems or routers, and should rarely be encountered by the daemon.

CVE-2016-1550, described as an NTP authentication potential timing vulnerability: a successful attack on a 128 bit key shared between coordinating systems would let the attacker spoof NTP packets (and therefore set the target system to the wrong time.

CVE-2016-1549 is an NTP ephemeral association sybil vulnerability: the protocol supports the creation of peer associations for systems to agree on a common reference time.

The problem? There's no limit to how many peers can share the same key, and that means if an attacker can discover the key, they can set up malicious peers. With enough malicious peers sharing the wrong time, they can “drown out” the correct time, the post says.

CVE-2016-1548 “Xleave pivot: NTP basic mode to interleaved”. The attacker can use this vulnerability to break the association between client and server, and impersonate the server to set the wrong time at the client.

CVE-2016-1547, “demobilization of preemptible associations”, is a denial-of-service vulnerability. The attacker can spoof the address of a machine in a crypto-NAK packet (that is, the recipient signalling that they were unable to authenticate the sender), and that breaks the association between peers in the system.

NTP Bug 2246

Summary: There is a bug affecting 3rd party GPS based NTP servers. If the servers are running code that does not have the fix for this bug, then the NTP server will send out the leap second flag at the end of every month. Those customers that have implemented the workaround may be affected on August 31.

Resolution: Fixed with version 5.2.1 update
Email from Dave Sohn (20 Aug 2015, referring to SecureSync/NetClock version 5.2.1 software) This appears to have been resolved in 4.2.8, which is in our latest released SW (5.2.1). 4.2.7 was the development branch of NTP, which led to 4.2.8.

13 NTP vulnerabilities identified (Oct 2015, v4.2.8p3 and below):

- Refer to kb article on our website: http://support.spectracomcorp.com/articles/FAQ/NTP-Vulnerabilities-Prior-to-Version-4-2-8p4?q=cve-2015&
- Refer to http://support.ntp.org/bin/view/Main/SecurityNotice and http://support.ntp.org/bin/view/Main/SecurityNotice#Recent_Vulnerabilities

NTF's NTP Project has been notified of the following 13 low- and medium-severity vulnerabilities that are fixed in ntp-4.2.8p4, released on Wednesday, 21 October 2015 (in descending order)

Work-arounds for 9200/9300 series

- Sample Draft email below for 9200s and 9300s since NTP isn’t being updated beyond version 4.2.0 (Keith sent to a customer 9 Dec 2015)

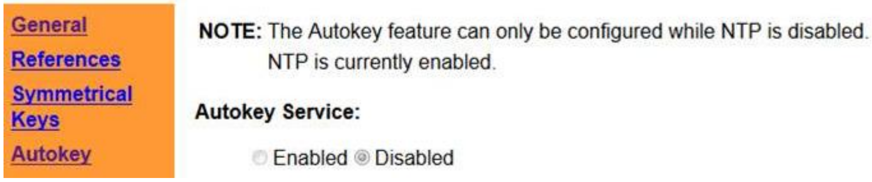
To begin, for additional information on the thirteen potential NTP vulnerabilities that were all announced at the same time please refer to the knowledge base article on our website: http://support.spectracomcorp.com/articles/FAQ/NTP-Vulnerabilities-Prior-to-Version-4-2-8p4?q=cve-2015&

In summary of the article, many of these potential NTP vulnerabilities are associated with the use of NTP Autokey (encryption) and NTP Symmetric Key (authentication). Most of the others are associated with NTPQ/NTPDC (available utilities/queries for NTP).

Note there is a link in the article ("for more information on NTP access restrictions") which will take you to a page discussing how to setup Access Restrictions in our newer SecureSync NTP time servers (which have replaced the Model 9300 and 9200 series NetClocks). The general information provided in this link also applies to the NetClock Model 9300s/9200s as well, but the configuration of this function is a little different in the 9300/9200s than in the SecureSyncs. Access Restriction configuration, specific to the Model 9300/9200s, is discussed further below for your reference.

Regarding "work-arounds" for the discontinued Model 9300 and 9200 series NetClocks, we recommend refraining from using NTP Autokey or Symmetric Key authentication with NTP clients. Note that NTP Autokey is very seldom used.

To verify that NTP Autokey is "Disabled" in the NetClock, navigate to the **NTP** -> **Autokey** page of the NetClock's web browser. As shown below, verify the "**Autokey Service**" is "Disabled" (If by a very small chance it's currently enabled, we recommend disabling it in the NetClock and in the NTP Clients).

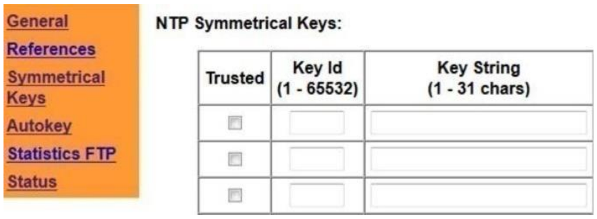


NOTE: The Autokey feature can only be configured while NTP is disabled.
NTP is currently enabled.

Autokey Service:

○ Enabled ● Disabled

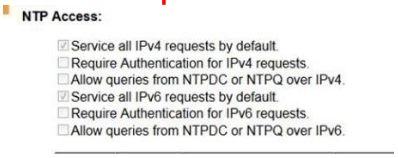
To see if Symmetric Key authentication is possibly being used with the NTP clients, navigate to the **NTP** -> **Symmetrical Keys** page of the NetClock's web browser. As shown below, if the table on this page is empty, Symmetric Key is not being used with the NTP clients.



NTP Symmetrical Keys:

Trusted	Key Id (1 - 65532)	Key String (1 - 31 chars)
□		
□		
□		

NTP Access Restriction:
We also highly recommend verifying that NTP queries for NTPQ/NTPDC (disabled by factory default) are still disabled in the NetClock. To verify the queries are disabled, navigate to the **NTP** -> **General** page of the NetClock's web browser. Scroll down to the checkboxes under "**NTP Access**": As shown below, verify the two checkboxes for **"Allow queries from NTPDC or NTPQ over IP4**" and **"Allow queries from NTPDC or NTPQ over IP6**" are **not** selected:



NTP Access:

☑ Service all IPv4 requests by default.
□ Require Authentication for IPv4 requests.
□ Allow queries from NTPDC or NTPQ over IPv4.
☑ Service all IPv6 requests by default.
□ Require Authentication for IPv6 requests.
□ Allow queries from NTPDC or NTPQ over IPv6.

NTP Access Restriction:

NTP Access Restriction for the Model 9383 is configured in the **NTP** ->**General** page of the browser (under "NTP Access"). Note that the NTP Service (**NTP** -> **General** page) needs to first be first be Disabled in order to make changes to the NTP configuration.

By default, all NTP clients have access to the NTP server to obtain NTP time stamps. If desired, access to NTP time stamps from the NetClock can be limited by IP address or subnet mask. This entails unselecting "**Service all IP4 requests by default"** (and also "**Service all IP4 requests by default"** if applicable). Then, adding entries to the table below the checkboxes which either "Allow" or "Deny" access to specific clients or subnets. If one entry is added to "allow" access, at that point all other NTP clients that are not at that IP address or in that subnet are thereby denied NTP access to the NetClock.

- Bug 2941 **CVE-2015-7871** NAK to the Future: Symmetric association authentication bypass via crypto-NAK (Cisco ASIG)

  Summary: Crypto-NAK packets can be used to cause ntpd to accept time from unauthenticated ephemeral symmetric peers by bypassing the authentication required to mobilize peer associations. This vulnerability appears to have been introduced in ntp-4.2.5p186 when the code handling mobilization of new passive symmetric associations (lines 1103-1165) was refactored.

Workaround for 9200/9300s: (don't use NTP symmetric key authentication)???
If you are unable to upgrade apply the patch to the bottom of the "authentic" check block around line 1136 of ntp_proto.c. Monitor your ntpd instances.

- Bug 2922 **CVE-2015-7855** decodenetnum() will ASSERT botch instead of returning FAIL on some bogus values (IDA)

Summary: If ntpd is fed a crafted mode 6 or mode 7 packet containing an unusually long data value where a network address is expected, the decodenetnum() function will abort with an assertion failure instead of simply returning a failure condition.

Workaround for 9200/9300s: don't enable Mode 7 packets. Use "restrict noquery" to limit who can send mode 6 and mode 7 requests.

- Bug 2921 **CVE-2015-7854** Password Length Memory Corruption Vulnerability. (Cisco TALOS)

Summary: If ntpd is configured to allow remote configuration, and if the (possibly spoofed) source IP address is allowed to send remote configuration requests, and if the attacker knows the remote configuration password or if ntpd was (foolishly) configured to disable authentication, then an attacker can send a set of packets to ntpd that may cause it to crash, with the hypothetical possibility of a small code injection.

Workaround for 9200/9300s: If you are unable to upgrade, remote configuration of NTF's ntpd requires:
Can explicitly configured "trusted" key. Only configure this if you need it. Access from a permitted IP address.
You choose the IPs. Authentication. Don't disable it. Practice secure key safety.

- Bug 2920 **CVE-2015-7853** Invalid length data provided by a custom refclock driver could cause a buffer overflow. (Cisco TALOS)

Summary: A negative value for the datalen parameter will overflow a data buffer. NTF's ntpd driver implementations **always set this value to 0 and are therefore not vulnerable to this weakness**. **If** you are running a custom refclock driver in ntpd and that driver supplies a negative value for datalen (no custom driver of even minimal competence would do this) then ntpd would overflow a data buffer. It is even hypothetically possible in this case that instead of simply crashing ntpd the attacker could effect a code injection attack.

Workaround for 9200/9300s:
If you are unable to upgrade:

- If you are running cust**o**m refclock drivers, make sure the signed datalen value is either zero or positive.

- Bug 2919 **CVE-2015-7852 ntpq atoascii() Memory Corruption Vulnerability. (Cisco TALOS)**

Summary: **If** an attacker can figure out the precise moment that ntpq is listening for data and the port number it is listening on or if the attacker can provide a malicious instance ntpd that victims will connect to then an attacker can send a set of crafted mode 6 response packets that, if received by ntpq, can cause ntpq to crash.

Workaround for 9200/9300s: If you are unable to upgrade and you run ntpq against a server and ntpq crashes, try again using raw mode. Build or get a patched ntpq and see if that fixes the problem.

- Bug 2918 **CVE-2015-7851 saveconfig Directory Traversal Vulnerability. (OpenVMS) (Cisco TALOS)**

Summary: **If** ntpd is configured to allow remote configuration, and if the (possibly spoofed) IP address is allowed to send remote configuration requests, and if the attacker knows the remote configuration password or if ntpd was configured to disable authentication, then an attacker can send a set of packets to ntpd that may cause ntpd to overwrite files.

Workaround for 9200/9300s: If you are unable to upgrade, remote configuration of NTF's ntpd requires:

- an explicitly configured "trusted" key. Only configure this if you need it.
- access from permitted IP addresses. You choose the IPs.
- authentication. Don't disable it. Practice key security safety.

- Bug 2917 **CVE-2015-7850** remote config logfile-keyfile. (Cisco TALOS)

  Summary: If ntpd is configured to allow remote configuration, and if the (possibly spoofed) source IP address is allowed to send remote configuration requests, and if the attacker knows the remote configuration password or if ntpd was configured to disable authentication, then an attacker can send a set of packets to ntpd that will cause it to crash and/or create a potentially huge log file. Specifically, the attacker could enable extended logging, point the key file at the log file, and cause what amounts to an infinite loop.

  Workaround for 9200/9300s: If you are unable to upgrade, remote configuration of NTF's ntpd requires:
  - an explicitly configured "trusted" key. Only configure this if you need it.
  - access from permitted IP addresses. You choose the IPs.
  - authentication. Don't disable it. Practice key security safety.

- Bug 2916 **CVE-2015-7849** trusted key use-after-free. (Cisco TALOS)

  Summary: **If** ntpd is configured to allow remote configuration, and if the (possibly spoofed) source IP address is allowed to send remote configuration requests, and if the attacker knows the remote configuration password or if ntpd was configured to disable authentication, then an attacker can send a set of packets to ntpd that may cause a crash or theoretically perform a code injection attack.

  Workaround for 9200/9300s: If you are unable to upgrade, remote configuration of NTF's ntpd requires:
  - an explicitly configured "trusted" key. Only configure this if you need it.
  - access from permitted IP addresses. You choose the IPs.
  - authentication. Don't disable it. Practice key security safety.

- Bug 2913 **CVE-2015-7848** mode 7 loop counter underrun. (Cisco TALOS)

  Summary: issues with Mode 7 packets
  Workaround for 9200/9300s: If you are unable to upgrade:
  - In ntp-4.2.8, mode 7 is disabled by default. Don't enable it.
  - If you must enable mode 7:
    - configure the use of a requestkey to control who can issue mode 7 requests.
    - configure restrict noquery to further limit mode 7 requests to trusted sources.

- Bug 2909 **CVE-2015-7701** Slow memory leak in CRYPTO_ASSOC. (Tenable)

  Summary: If ntpd is configured to use autokey, then an attacker can send packets to ntpd that will, after several days of ongoing attack, cause it to run out of memory.
  Workaround for 9200/9300s: Don't use NTP Autokey

- Bug 2902: **CVE-2015-7703** configuration directives "pidfile" and "driftfile" should only be allowed locally. (RedHat)

  Summary: If ntpd is configured to allow for remote configuration, and if the (possibly spoofed) source IP address is allowed to send remote configuration requests, and if the attacker knows the remote configuration password, it's possible for an attacker to use the "pidfile" or "driftfile" directives to potentially overwrite other files.

  Workaround for 9200/9300s: don't enable remote configuration/queries.

- Bug 2901: **CVE-2015-7704**, **CVE-2015-7705** Clients that receive a KoD should validate the origin timestamp field. (Boston University)

  Summary: An ntpd client that honors Kiss-of-Death responses will honor KoD messages that have been forged by an attacker, causing it to delay or stop querying its servers for time updates. Also, an attacker can forge packets that claim to be from the target and send them to servers often enough that a server that implements KoD rate limiting will send the target machine a KoD response to attempt to reduce the rate of incoming packets, or it may also trigger a firewall block at the server for packets from the target machine. For either of these attacks to succeed, the attacker must know what servers the target is communicating with. An attacker can be anywhere on the Internet and can frequently learn the identity of the target's time source by sending the target a time query.

  Workaround for 9200/9300s: “If you can't upgrade, restrict who can query ntpd to learn who its servers are, and what IPs are allowed to ask your system for the time

- Bug 2899: **CVE-2015-7691, CVE-2015-7692, CVE-2015-7702** Incomplete autokey data packet length checks. (Tenable)

  Workaround for 9200/9300s: Don’t use NTP autokey

The only generally-exploitable bug in the above list is the crypto-NAK bug, which has a CVSS2 score of 6.4.

Additionally, three bugs that have already been fixed in ntp-4.2.8 but were not fixed in ntp-4.2.6 as it was EOL'd have a security component, but are all below 1.8 CVSS score, so we're reporting them here:

- Bug 2382: Peer precision < -31 gives division by zero
- Bug 1774: Segfaults if cryptostats enabled when built without OpenSSL
- Bug 1593: ntpd abort in free() with logconfig syntax error

Products (for all 13 CVE’s and 3 additions bugs listed above

- ○ **1200 SecureSync/9400s**

  Software versions 5.3.0 and below (version 5.3.0 updated NTP to version 4.2.8p3)

- ○ **NetClock 9300 and 9200 series:**

  At least software versions 3.6.7 and below (all versions are at NTP version 4.2.0)

CVE-2015-5146 (ntpd control message crash: Crafted NUL-byte in configuration directive)

- ➢ Refer to sites such as http://support.ntp.org/bin/view/Main/SecurityNotice#June_2015_NTP_Security_Vulnerabi or
- ➢ https://access.redhat.com/security/cve/CVE-2015-5146
- ➢ Applies to NTPv4.2.8p2 and below (SecureSync/NetClock 9400 versions 5.2.1 and below)
- ➢ NTP was updated to 4.2.8p3 with the version 5.3.0 software update
- ➢ Fix- update software to version 5.3.0 or higher
- ➢ Temporary work-around: make sure NTP queries (NTPD and NTPDC) are still disabled (disabled by default)

Summary: Under limited and specific circumstances an attacker can send a crafted packet to cause a vulnerable ntpd instance to crash. This requires each of the following to be true:

1. **ntpd set up to allow for remote configuration (not allowed by default), and**
2. **knowledge of the configuration password, and**
3. **access to a computer entrusted to perform remote configuration.**

Products (Note: only when using NTP symmetric key**)**

- ○ **1200 SecureSync/9400s**

  Software versions 5.2.1 and below (version 5.3.0 updated NTP to version 4.2.8p3).

- ○ **NetClock 9300 and 9200 series:**

  At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0)

CVE-2015-1799 (NTP Symmetric Key)

The symmetric-key feature in the receive function in ntp_proto.c in ntpd in NTP 3.x and 4.x before 4.2.8p2 performs state-variable updates upon receiving certain invalid packets,

- ➢ NTP versions before 4.2.8p2
- ➢ NTP Symmetric key mode only (N/A if not using symmetric key)

Products (Note: only when using NTP symmetric key**)**

- ○ **1200 SecureSync/9400s**

  Software versions 5.2.0 and below (version 5.2.1 updated NTP to version 4.2.8p2)

- ○ **NetClock 9300 and 9200 series:**

  At least software versions 3.6.7 and below (at least 3.6.7 and below are all at NTP v4.2.0).

CVE-2015-1798 (NTP Symmetric Key)

The symmetric-key feature in the receive function in ntp_proto.c in ntpd in NTP 4.x before 4.2.8p2 requires a correct MAC only if the MAC field has a nonzero length

- ➢ NTP versions before 4.2.8p2
- ➢ NTP Symmetric key mode only (N/A if not using symmetric key)

Products: (Note: only when using NTP symmetric key**)**

- ○ **1200 SecureSync/9400s**

  Software versions 5.2.0 and below (version 5.2.1 updated NTP to version 4.2.8p2)

- ○ **NetClock 9300 and 9200 series**

  At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0)

CVE-2014-9296

The receive function in ntp_proto.c in ntpd in NTP before 4.2.8 continues to execute after detecting a certain authentication error, which might allow remote attackers to trigger an unintended association change via crafted packets.

- ➢ NTP versions before 4.2.8

Products:

- ○ **1200 SecureSync/9400s:**

  Software versions 5.2.0 and below (version 5.2.1 updated NTP to version 4.2.8p2)

- ○ **NetClock 9300 and 9200 series**

  At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0)

CVE-2014-9295 (NTP Autokey)

Multiple stack-based buffer overflows in ntpd in NTP before 4.2.8 allow remote attackers to execute arbitrary code via a crafted packet, related to (1) the crypto_recv function when the Autokey Authentication feature is used.

- ➢ NTP versions before 4.2.8
- ➢ **Work-around**: Verify NTP Autokey is still disabled (disabled by default)

Products: (Note: only applicable if NTP Autokey has been enabled)

- ○ **1200 SecureSync/9400s**

  Software versions 5.2.0 and below (version 5.2.1 updated NTP to version 4.2.8p2)

- ○ **NetClock 9300 and 9200 series**

  At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0)
  Don't use NTP autokey

CVE-2014-9294

util/ntp-keygen.c in ntp-keygen in NTP before 4.2.7p230 uses a weak RNG seed, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via a brute-force attack.

- ➢ NTP versions before 4.2.7p230

Products:

- ○ **1200 SecureSync/9400s:**

  Software versions 5.2.0 and below (version 5.2.1 updated NTP to version 4.2.8p2)

- ○ **NetClock 9300 and 9200 series**

  At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0)

CVE-2014-9293

The config_auth function in ntpd in NTP before 4.2.7p11, when an auth key is not configured, improperly generates a key, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via a brute-force attack.

- ➢ NTP versions before 4.2.7p11

Products:

- ○ **1200 SecureSync/9400s**

  Software versions 5.2.0 and below (version 5.2.1 updated NTP to version 4.2.8p2)

- ○ **NetClock 9300 and 9200 series**

  At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0)

CVE-2013-5211 (Monlist in NTPDC)

The monlist feature in ntp_request.c in ntpd in NTP before 4.2.7p26 allows remote attackers to cause a denial of service (traffic amplification) via forged (1) REQ_MON_GETLIST or (2) REQ_MON_GETLIST_1 requests

- ➢ NTP versions before 4.2.7p26

Products:

- ○ **1200 SecureSync/9400s**

  Software versions 5.2.0 and below are affected (version 5.2.1 updated NTP to version 4.2.8p2)

- ○ **NetClock 9300 and 9200 series**

  At least software versions 3.6.7 and below are affected (at least 3.6.7 and below are at NTP version 4.2.0)

CVE-2009-3563
ntp_request.c in ntpd in NTP before 4.2.4p8, and 4.2.5, allows remote attackers to cause a denial of service

- NTP versions before 4.2.4p8

Products:

- **Legacy VelaSyncs**
- **1200 SecureSync/9400s**

  Software versions 4.8.9 and below are affected (version 5.0.0 updated NTP to version 4.2.6)

- **NetClock 9300 and 9200 series**

  At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0)

CVE-2009-1252 (NTP Autokey)
Stack-based buffer overflow in the crypto_recv function in ntp_crypto.c in ntpd in NTP before 4.2.4p7 and 4.2.5 before 4.2.5p74, when OpenSSL and autokey are enabled, allows remote attackers to execute arbitrary code via a crafted packet containing an extension field.

- Refer to https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1252 and http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1252
- NTP versions before 4.2.4p7
- **Work-around:** Verify NTP Autokey is still disabled (disabled by default)

Products: (Note: only applicable if NTP Autokey has been enabled)

- **1200 SecureSync/9400s**

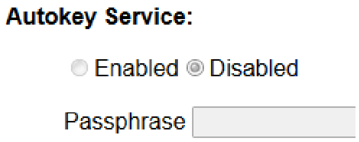
  Software versions 4.8.9 and below (version 5.0.0 updated NTP to version 4.2.6)

- **NetClock 9300 and 9200 series**

  At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0)

Email Keith sent to Adnet (27 Apr 15) for 9383
To begin and specific to this this potential vulnerability, it is associated with NTP Autokey mode only. NTP Autokey is a very unique mode of NTP that is seldom used. If NTP autokey is not being used on all of the NTP servers and NTP clients on the network, this potential vulnerability can be disregarded as it does not apply to standard operation of NTP. (from the website of http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1252, “when **OpenSSL and autokey are enabled**, allows remote attackers to execute arbitrary code via a crafted packet containing an extension field”).

The mitigation for this potential vulnerability is to leave NTP autokey disabled (factory default configuration). NTP Autokey being Disabled can be verified via the **NTP** -> **Autokey** page of the NetClock’s web browser, as shown below:



Autokey Service:

○ Enabled ● Disabled

Passphrase

In general, about the NTP version installed in the NetClocks, the Spectracom Model 9383 is a discontinued product. It has been replaced by the SecureSync time servers. Because the Model 9383 is a discontinued product, there are no plans at this time for NTP to be updated to a newer version in this earlier Model time server. To be able to implement newer versions of NTP, I recommend replacing the discontinued Model 9383 with a SecureSync.

Our Sales team can provide you with information on the SecureSync, as needed.

CVE-2009-0159 (NTPQ/NTPDC)
Stack-based buffer overflow in the cookedprint function in ntpq/ntpq.c in ntpq in NTP before 4.2.4p7-RC2 allows remote NTP servers to execute arbitrary code via a crafted response

- ➢ NTP versions before 4.2.4p7
- ➢ **Work-around:** disable NTP queries (NTPD/NTPDC) in the web browser (disabled by default)

Products: (Note: only applicable if NTP queries has been enabled)

- ○ **1200 SecureSync/9400s**

  Software versions 4.8.9 and below (version 5.0.0 updated NTP to version 4.2.6)

- ○ **NetClock 9300 and 9200 series**

  At least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0)

CVE-2009-0021

NTP 4.2.4 before 4.2.4p5 and 4.2.5 before 4.2.5p150 does not properly check the return value from the OpenSSL EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys

- ➢ NTP v4.2.4 before 4.2.4p5 and 4.2.5 before 4.2.5p150

Products:

- ○ **1200 SecureSync/9400s:**

  Software versions 4.8.9 and below (version 5.0.0 updated NTP to version 4.2.6)

- ○ **NetClock 9300 and 9200 series**

  With at least software versions 3.6.7 and below (at least 3.6.7 and below are at NTP version 4.2.0)

CVE-2004-0657

- ➢ NTP before 4.0.0

Products: None **(**NTP versions before 4.0.0 so not applicable to 9200s, 9300s, 9400s or SecureSync)

NOTE: END of **NTP-Specific** vulnerabilities

****Debian vulnerabilites (Model 1232 VelaSync OS)

- Table below is from Salesforce Case 219165 (with version 1.2.0 installed)
- Comments are from Julian Beraud (Engineer) 24 Jan 2020

CVE	Comments
Debian: CVE-2016-10150: linux – security update	Affects kernel 4.8.13 – Doesn't affect 4.9.0-7-amd64 present on Velasync
Debian: CVE-2019-15292: linux, linux-4.9 -- security update	affects the appletalk driver, no such hardare on the Velasync
Debian: CVE-2019-15926: linux, linux-4.9 -- security update	affects the atheros 6k wireless driver, no such hardware on Velasync
Debian: CVE-2019-14287: sudo -- security update	affects sudo with some specific permissions, no impact on Velasync
Debian: CVE-2019-11815: linux, linux-4.9 -- security update	affects rds, not used on Velasync
Debian: CVE-2018-20836: linux, linux-4.9 -- security update	affects the sas_expander driver, no such hardware on Velasync
Debian: CVE-2019-12735: neovim, vim -- security update	affects vim and neovim. Not installed on Velasync
Debian: CVE-2019-12735: neovim, vim -- security update	affects vim and neovim. Not installed on Velasync
Debian: CVE-2018-14633: linux, linux-4.9 -- security update	affects iscsi, not enabled on Velasync
Debian: CVE-2018-14882: tcpdump -- security update	Affects tcpdump. Proposed mitigation: don't use tcpdump (not used by the system)
Debian: CVE-2018-14470: tcpdump -- security update	
Debian: CVE-2018-14461: tcpdump -- security update	
Debian: CVE-2018-14464: tcpdump -- security update	
Debian: CVE-2018-16230: tcpdump -- security update	
Debian: CVE-2018-16227: tcpdump -- security update	
Debian: CVE-2018-16229: tcpdump -- security update	
Debian: CVE-2018-16451: tcpdump -- security update	
Debian: CVE-2019-15166: tcpdump -- security update	
Debian: CVE-2018-10103: tcpdump -- security update	
Debian: CVE-2019-18218: file -- security update	Affects the « file » utility. Not installed on Velasync
Debian: CVE-2018-14462: tcpdump -- security update	Same as upwards. Don't use tcpdump
Debian: CVE-2018-14467: tcpdump -- security update	
Debian: CVE-2018-10105: tcpdump -- security update	
Debian: CVE-2019-11043: php5, php7.0, php7.3 - security update	Affects php-fpm. Not installed on Velasync
Debian: CVE-2019-3846: linux, linux-4.9 -- security update	affects mwifiex driver. No such hardware on Velasync
Debian: CVE-2018-14881: tcpdump -- security update	Same as upwards. Don't use tcpdump
Debian: CVE-2018-14879: tcpdump -- security update	
Debian: CVE-2018-14466: tcpdump -- security update	
Debian: CVE-2019-10126: linux, linux-4.9 -- security update	affects mwifiex driver. No such hardware on Velasync
Debian: CVE-2018-14880: tcpdump -- security update	Same as upwards. Don't use tcpdump
Debian: CVE-2018-14463: tcpdump -- security update	
Debian: CVE-2018-14465: tcpdump -- security update	

Debian: CVE-2018-14468: tcpdump -- security update	
Debian: CVE-2018-14469: tcpdump -- security update	
Debian: CVE-2018-16228: tcpdump -- security update	

All other vulnerabilities (not associated with NTP or Debian)

CWE's: The Common Weakness Enumeration numbers (such as CWE#20, for example)

- Per Paul Myers, (CWE™) is a list of software weaknesses types. Creating the list is a community initiative aimed at creating specific and succinct definitions for each common weakness type.

QID*:* The unique **Qualys** ID number assigned to the vulnerability.

(listed in descending order)

CWE-918: Server-Side Request Forgery (SSRF) (Also called XSPA, Cross Site Port Attack)

1. The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS). QID Detection Logic: This QID (38003) **detects the absence of the Content-Security-Policy HTTP header** by transmitting a GET request.

SecureSyncs

- Appears to Keith to be a report that HSTS functionality is not enabled in SecureSyncs?
- Refer to Salesforce Case **258190**
- Refer to JIRA **SSS-1120**
- Found in versions 5.9.0 and 5.9.1 (Report 15 Feb 2021)
- Refer to: https://cwe.mitre.org/data/definitions/918.html (excerpt below)

  The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

CWE-601: URL Redirection to Untrusted Site ('Open Redirect', "Cross-site Redirect", Cross-domain Redirect")

- QID-11827 (HTTP Security Header Not Detected)

2. HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates. QID Detection Logic: This QID (11827) detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

SecureSyncs

- Appears to Keith to be a report that HSTS functionality is not enabled in SecureSyncs?
- Refer to Salesforce Case **258190**
- Refer to JIRA **SSS-1121**
- Found in versions 5.9.0 and 5.9.1 (Report 15 Feb 2021)
- Refer to: https://cwe.mitre.org/data/definitions/601.html

  A web application accepts a user-controlled input that specifies a link to an external site, and uses that link in a Redirect. This simplifies phishing attacks.

Apache Struts and Apache Tomcat (AKA “Tomcat Server”)
SecureSyncs

- As of at least version 5.7.1 (~Oct 2017) neither of these add-on programs (Apache Struts or Apache Tomcat server) are used in SecureSyncs/9400s, as confirmed by Engineering, and are **not likely** to start being used anytime in the future.
- Any potential vulnerabilities directly associated with these available add-on programs do not apply.

Email from Paul Myers (16 Mar 17)

https://struts.apache.org/
We don’t include apache struts.
I don’t see apache struts as part of Gentoo anyway.
We use apache web server.

Email from Ron Dries (16 Oct 17) Correct, SecureSync does not use Apache Tomcat.

"SSH Weak MACs/SSH Weak Message Authentication Code Algorithms"

- Refer to sites such as https://www.rapid7.com/db/vulnerabilities/ssh-weak-message-authentication-code-algorithms/#:~:text=The%20SSH%20server%20supports%20cryptographically%20weak%20Hash-based%20message,Hash-based%20algorithms.%20Advanced%20vulnerability%20management%20analytics%20and%20reporting.

  https://www.virtuesecurity.com/kb/ssh-weak-mac-algorithms-enabled/

Description The SSH server supports cryptographically weak Hash-based message authentication codes (HMACs) including MD5 or 96-bit Hash-based algorithms.

What are SSH Weak MAC Algorithms?

As with most encryption schemes, SSH MAC algorithms are used to validate data integrity and authenticity. A ‘MAC algorithm’ should not be conflated with a MAC (Message Authentication Code) as these are two distinct components. The MAC *algorithm* uses a message and private key to generate the fixed length MAC.

MAC algorithms may be considered weak for the following reasons:

1. A known weak hashing function is used (MD5)
2. The digest length is too small (Less than 128 bits)
3. The tag size is too small (Less than 128 bits)

Example of Known Weak MAC Algorithms

The following are the most common weak MAC algorithms encountered**:**

md5
md5-96
sha1-96
sha2-256-96
sha2-512-96

- **1200 SecureSyncs**

  - Refer to Salesforce Case **282790**/JIRA **SSS-1258**

    A 1200 SecureSync hotpatch was created for Wegmans, v5.9.4, to remove these undesired ciphers from 1200 SecureSyncs. The patch is in the JIRA ticket **SSS-1258** and also in: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software patches\Disable SSH ciphers (Wegmans JIRA SSS-1258) Note this patch was tested on 2400 SecureSyncs and does not work.

- **2400 SecureSyncs**

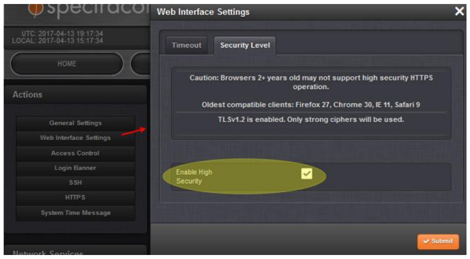
  - Refer to Salesforce Case **287015**/JIRA ticket **DMND-1841**

SSL - Server Supports Weak SSL Cipher

SecureSyncs

1) Make sure Classic Interface Web Browser is not enabled (or update to at least version 5.9.1 to completely remove it)
2) Enable High Security (Hi-Sec) to disable earlier versions of TLS. Refer to "**Disabling TLS**" in online SecureSync user guide at: http://manuals.spectracom.com/SS/Content/KB/TLSdisable.htm

   - Click "**Web interface Settings**" on the left side of the **Management** -> **Network Setup** page of the browser, and select the **Security Level** tab. Then select the "**Enable High Security"** checkbox to disable the referenced ciphers and press Submit.



Caution: Browsers 2+ years old may not support high security HTTPS operation.

Oldest compatible clients: Firefox 27, Chrome 30, IE 11, Safari 9

TLSv1.2 is enabled. Only strong ciphers will be used.

Enable High Security ☑

CGI Generic SQL Injection (CWE#20, CWE#77, CWE#751, CWE#722, CWE#91, CWE#203, CWE#643, CWE#713, CWE#801, CWE#89, CWE#928, CWE#929")

- Refer to Salesforce case 25183
  - "Our vulnerability scanner scanned our Spectracom Secure Sync box and found a vulnerability related to SQL Injection on the management IP. The vulnerability references are CWE#20, CWE#77, CWE#751, CWE#722, CWE#91, CWE#203, CWE#643, CWE#713, CWE#801, CWE#89, CWE#928, CWE#929"
- Refer to sites such as: http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- Ability to directly edit an SQL database entry???

Products:

- **Legacy VelaSync: ???**
- **1200 SecureSync/9400s:** ????
- **NetClock 9300 and 9200 series**: Software versions 3.6.7 and below???

Email from Paul (28 Apr 17) Case 25183 Action items:
1. Customer Service must find the tool they are using to identify CWE.
2. Engineering will write JIRA ticket to determine how to scan/identify CWE effects in software we write and determine how/should we fix them.

The Classic Web UI does NOT to my knowledge use SQL. It is a web ui that existed before the New Web UI which used SQL.

I believe this is a new scanning technique to look for software defects/vulnerabilities in written software not packages used in software like Linux or web pages. The application developer writes code such as our PHP which can be evaluated to issues and vulnerabilities. This appears to be a scan tool that evaluates our web pages we have written.

See
https://cwe.mitre.org/data/index.html

http://www.securiteam.com/securityreviews/5DP0N1P76E.html

The vulnerability references are CWE#20, CWE#77, CWE#751, CWE#722, CWE#91, CWE#203, CWE#643, CWE#713, CWE#801, CWE#89, CWE#928, CWE#929

The Common Weakness Enumeration (CWE™) is a list of software weaknesses types. Creating the list is a community initiative aimed at creating specific and succinct definitions for each common weakness type.
This is an effort to assist software developers in writing more secure software in this case web pages.

This scan result is ASSUMED to be looking at our New Web UI code and identifying software techniques that might be or might be INTERPRETED as being areas of risk to security. It is NOT clear if these are actual exploits.

I am creating a JIRA Ticket to evaluate these, however, they may NOT be software defects.

The customer is running Release 5.1.7 which is very old.
I recommend they update to 5.6.0 or 5.7.0 which may have the same or more issues, but unless we can add a CWE scanning tool our tool set we cannot find our own defects.

Several SecureSync "design" vulnerabilities (no CVE numbers assigned) listed below (all reported at same time)

- ➢ Refer to salesforce case number **25403** for Roots in Asia
  - ○ **Note: version 5.6.0 and then 5.7.0** software installed was installed at the time they were all reported.

1) No authentication for single user mode (lilo-linux-single-user-mode) (see table below)

2) ICMP redirection enabled (linux-icmp-redirect)

3) No password for Grub (linux-grub-missing-passwd)

4) Weak permissions for Password, Shadow and Group Files (generic-passwd-shadow-group-file-permissions) (see table below)

5) World writable files exist (unix-world-writable-files) (see table below)

6) ICMP timestamp response (generic-icmp-timestamp)

7) TCP timestamp response (generic-tcp-timestamp)

8) User home directory mode unsafe (see table below)

No.	Risk	Justification
	Severe Vulnerabilities	
1	No authentication for single user mode (lilo-linux-single-user-mode)	Access to single user mode currently requires internal physical access to the unit, including removal of the top cover, as no external connections can break into the boot process. Physical security has been considered a requirement of the end user, however, we will add password protection as a release ticket.
2	Weak permissions for Password, Shadow and Group Files (generic-passwd-shadow-group-file-permissions)	Permissions are currently as follows: -rw-r--r-- 1 root root 739 May 31 14:42 /etc/group -rw-r--r-- 1 root root 1696 May 31 14:42 /etc/passwd -rw-r----- 1 root root 726 May 31 14:42 /etc/shadow A shadow permissions setting of 640 vs 400 is required to support web UI login mechanisms with local authentication.
3	World writable files exist (unix-world-writable-files)	A few files listed as world writable, while low risk, will be marked with a release ticket to resolve. The remaining files are intended as world writable as they are intended as user configurable to support language and UI customizations available for configuration for all users.
	Moderate Vulnerabilities	
4	User home directory mode unsafe (unix-user-home-dir-mode)	This will remain as it is, so that customer can access the site to perform software upgrades. This directory requiring successful login to be able to access it, making this directory locked-down would inhibit everyone from being able to apply software updates in the field

WebDAV Extensions are Enabled (http-generic-webdav-enabled)

- ➢ Found in a SecureSync with version 4.7.0 software
- ➢ **Refer to** Mantis case 1595

- Also reported in a v5.8.8 scan (refer to Salesforce Case 258597) Suspect the classic interface browser has been enabled (disable classic interface or update to at least version 5.9.1, which completely removes the classis interface browser).

Description:
WebDAV is a set of extensions to the HTTP protocol that allows users to collaboratively edit and manage files on remote web servers. Many web servers enable WebDAV extensions by default, even when they are not needed. Because of its added complexity, it is considered good practice to disable WebDAV if it is not currently in use.

Reported solution:
Apache:

- Disable WebDAV for Apache
- Make sure the mod_dav module is disabled, or ensure that authentication is required on directories where DAV is required.

Keith's response (Feb 2021): It appears they likely have enabled the classic interface web browser. The classic web browser needs to be disabled (or update to 5.9.1 which will completely remove this 1st generation web browser).

If the classic interface is DISABLED already, please ask them to forward you a copy of the actual scan report. I haven't seen this one reported since version 4.7.0.

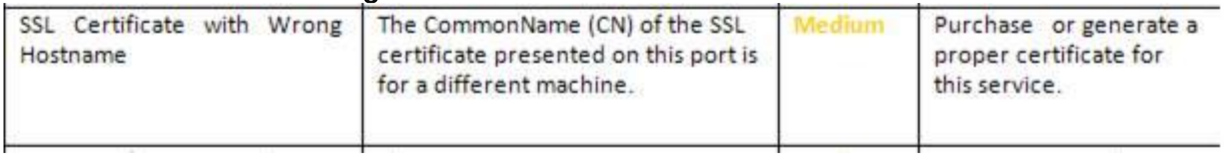
FTP server does not support AUTH command (ftp-generic-0007)

- Found in a SecureSync with version 4.7.0 software
- **Refer to** Mantis case 1595

Description: FTP clients send credentials (user ID and password) in clear text to the FTP server by default. This allows malicious users to intercept the credentials if they can eavesdrop on the connection. Newer FTP servers support the AUTH command, which provides enhanced authentication options such as TLS, Kerberos, GSSAPI, etc. This should be used to prevent eavesdropping on FTP connections.

Vulnerability Solution: Upgrade/migrate to an FTP server that supports the AUTH command.

SSL Certificate with Wrong Hostname



SSL Certificate with Wrong Hostname	The CommonName (CN) of the SSL certificate presented on this port is for a different machine.	Medium	Purchase or generate a proper certificate for this service.

Spectracom provides a default HTTPS certificate to alleviate the need to always purchase a certificate from an outside Certificate Authority (CA). The default HTTPS certificate uses the DNS hostname of Spectracom. Unless the host name is still Spectracom and you use the assigned DNS host name to access the web browser, a new HTTPS certificate will need to be created (either using the above recommendations of using an external CA or create your own new self-signed certificate, which will cause the above Vulnerability to still be reported). When generating this new HTTPS certificate, the value you enter to access the web browser (preferably the DNS host name), has to entered as part of the new certificate. The scanners prefer you use the DNS host name to login and not the assigned IP address that is assigned to the NTP server, though the scanner may accept the certificate using the IP address.

As the IP address and likely the DNS host name are network and customer-specific, we cannot use your values in the default Spectracom signed certificate. This requires you to create your own certificate in the NTP server and delete the default Spectracom certificate.

Attached is a document that discusses how to replace the default HTTPS certificate with a new self-signed certificate. Just keep in mind this process will not allow the previous vulnerability to be cleared. When creating the new certificate, make sure to enter the value that you use to access the web browser.

Possible Scan interference (“QID 42432 - Possible Scan Interference”)

- **Category**: General remote services
- No CVE ID assigned
- Observed with scan of SecureSync v5.5.0
- Refer to sites such as https://community.qualys.com/thread/13237

“QID 42432 Possible Scan Interference was recently added to Qualys due to increased focus by the PCI Council. The detection is usually triggered when no http services are identified on common web service ports, such as 80 & 443 (you can confirm by checking to see if service is listed as “Unknown” as part of QID 82023 Open TCP Services List in your scan results).”

Web Server Vendor / Version Disclosure

Summary of the info below: A customer requested the Apache version no longer be reported. Knowing the version installed could disclose potential vulnerabilities.

Vulnerability Explanation
A typical web server response contains an HTTP Server header that reveals both the vendor and the version of the web server software. Additionally, third parties may inject headers disclosing supported software such as PHP or ASP. This information can lead an attacker to more focused attacks.

Remediation - NTP not a windows box, will need to ask spectrum
Sequris Group recommends that SRPMIC scrub the response headers before they are returned to the user. Microsoft has released a utility (URLScan) that helps modify headers before being sent to the requesting client. Please see the following URL for additional details:
http://www.iis.net/downloads/microsoft/urlscan

OR

Can Spectracom edit the host file or related file on the Spectracom device to change or hide vendor information?

Email from Paul Myers (6 Mar 17) regarding SecureSyncs/9400s (at least 5.5.1 and below) In regards to hiding the Apache web server version information, we are reviewing this security recommendation internally with the Product Manager to see if we can fix this via Apache configuration in a future release.

“Missing HttpOnly Flag From Cookie” / “Missing Secure Flag From SSL Cookie”

A) SecureSyncs/9400s

- Refer to JIRA ticket **SSS-603** (addressed in 5.8.5 and above)
  - Per the Engineering Release Notes for v5.8.5: “* [SSS-603] “Set the SECURE and HTTPOnly attributes to cookies”
- Note there is no CVE number assigned to either of these vulnerabilities.
- reported in customer scan of v5.8.2
- Refer to sites such as: http://www.ietf.org/rfc/rfc2965.txt and https://www.owasp.org/index.php/Testing_for_cookies_attributes_%28OWASP-SM-002%29

Email from Danny Loke (8 Jan 2019) to Dave S This case is the same as "Security scans support case 164789". I had abstracted a part of their audited report, attached herein, SecureSync firmware version is V5.8.2

1) Missing HttpOnly Flag From Cookie

Resolution: Add the HttpOnly to all cookies

Configuration remediation steps
For each cookie generated by your web-site, add the "HttpOnly" flag to the cookie. For example:

Set-Cookie: <name>=<value>[; <Max-Age>=<age>]

```
[; expires=<date>][; domain=<domain_name>]
[; path=<some_path>][; secure][; HttpOnly]
```

2) Missing Secure Flag From SSL Cookie

Resolution: Add the Secure flag to cookies sent over SSL

Configuration remediation steps

For each cookie sent over SSL in your web-site, add the "Secure" flag to the cookie. For example:

```
Set-Cookie: <name>=<value>[; <Max-Age>=<age>]
    [; expires=<date>][; domain=<domain_name>]
    [; path=<some_path>][; secure][; HttpOnly]
```

Are these something we will implement in our next next firmware upgrade?

"HSTS Missing from HTTPS Server (RFC 6797)"

- Refer to "**HTTP / HSTS (HTTP Strict Transport Security)"** Section in I:\Customer Service\1- Cust Assist documents\SecureSync CustAssist.pdf

Publicly Exposed SQLite DB

It was discovered that it is possible to get SQLite3 DB file form the web applications. File contains information about locally configured user accounts, performance statistic and more. It does not represent direct risk of system compromise, but it gives a lot of information for future attacks planning.

- Observed with SecureSync v5.9.1 (Refer to Salesforce Case 276510)
- Refer to JIRA ticket CAR-1231 (for 2400s and 1200s)

Missing HSTS Headers

Web application does not implement the HTTP Strict Transport Security (HSTS) Header.

- Observed with SecureSync v5.9.1 (Refer to Salesforce Case 276510)

Missing Brute-Force Protection

It is possible to perform the brute-force attack to web application authentication schema by repeating the request on previous finding (HSTS header).

- Observed with SecureSync v5.9.1 (Refer to Salesforce Case 276510)

Host Header Injection Web application does not correctly handle the Host header value.

It does not validate the value and using it for link generation.

- Observed with SecureSync v5.9.1 (Refer to Salesforce Case 276510)

SuperMicro-related vulnerabilities

- **Supermicro sites regarding potential security vulnerabilities of their products:**
  - **Security Advisory:** https://www.supermicro.com/support/security_BMC_virtual_media.cfm
  - **Security Vulnerabilities Table:** https://www.supermicro.com/support/security_Intel-SA.cfm

A) September 2019 potential vulnerabilities: Baseboard Management Controller (BMC) component of Supermicro X9, X10, and X11 platforms

- Refer to cases such as 207858 (Sept 2019)
- Refer to sites such as https://www.us-cert.gov/ncas/current-activity/2019/09/04/supermicro-releases-security-updates

"Supermicro has released security updates to address vulnerabilities affecting the Baseboard Management Controller (BMC) component of Supermicro X9, X10, and X11 platforms. A remote attacker could exploit some of these vulnerabilities to take control of an affected system.
The Cybersecurity and Infrastructure Security Agency (CISA) encourages administrators to review Supermicro's Security Advisory and Security Vulnerabilities Table and apply the necessary updates and recommended mitigations.?

below is from: https://usgov.info/2019/09/04/supermicro-releases-security-updates/

"The Cybersecurity and Infrastructure Security Agency (CISA) encourages administrators to review Supermicro's Security Advisory and Security Vulnerabilities Table and apply the necessary updates and recommended mitigations."

Products:

- **1232 VelaSyncs:** This is a Supermicro device and thus MIGHT be affected (need to confer with Engineering)?
- **Legacy 1225 VelaSync:** This is a Supermicro device and thus MIGHT be affected **(need to confer with** Engineering)???
- **VersaSyncs:** N/A
- **1200 SecureSync/9400s:** N/A (see example email below sent to a customer)

  Email from Dave L (6 Sept 2019) No, the SecureSync platform is not built on Supermicro. Only our Velasync Products use Supermicro. Your Securesyncs are not affected by this issue.
- **NetClock 9300 and 9200 series**: N/A

"Apache 2.4.x < 2.4.54 Multiple Vulnerabilities" (~Sept 2022)

- **CVE's included: CVE-2022-28614 CVE-2022-28615 CVE-2022-26377 CVE-2022-28330 CVE-2022-29404 CVE-2022-30522 CVE-2022-CVE 2022-31813**
- **Fix is to update Apache to 2.4.54 or higher**
- **Refer to sites such as: https://www.tenable.com/plugins/nessus/161948**

Products:

- **2400 SecureSyncs**

2400 S/S Version	**Apache version**
1.6.0	**Still 2.4.54**
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1200 SecureSync/9400s:**

S/S Version	**Apache version**
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- Affects versions **5.9.5 and below** (expected to be addressed in **5.9.6** update, ~ beginning of 2023)
- Refer to Salesforce Cases such as 289252 and 267843
- Refer to JIRA tickets **SSS-1293** (excerpt below) and **SSS-1294**

From Gary Boff (5 Oct 2022)

@Ryan Johnson @Keith Wing here is the analysis results that @Tim Hammer documented in an email dated 7/29/2022:

RE: **267843** / SSS-1293 – FBI scan found CVEs on 5.9.5

- **CVE-2022-28614** – "modules compiled and distributed separately from Apache using ap_rwrite() or ap_rputs(),"
  other than PHP, I am not aware of any modules not provided by Apache; but I can cannot say with 100% confidence whether SS1200 is affected or not
  Severity score (NVD.NIST): Medium *(so I suspect we would not cut a release just for this issue)*
- **CVE-2022-28615** – "third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected"
  other than PHP, I am not aware of any modules not provided by Apache; but I can cannot say with 100% confidence whether SS1200 is affected or not
  Severity score (NVD.NIST): **Critical**
- **CVE-2022-26377** – mod_proxy_ajp
  *SS1200 does not use this module, so is **not affected***
- **CVE-2022-28330** – "on Windows"
  *it is not clarified anywhere that I can find, but I am going to assume this means "Microsoft Windows", and thus SS1200 is **not affected***
- **CVE-2022-29404** – "malicious request to a lua script that calls r:parsebody(0) may cause a denial of service"
  *SS1200 does have lua installed, so is **not affected***
- **CVE-2022-30522** – "mod_sed may make excessively large memory allocations and trigger an abort"
  *SS1200 does include this module, but I cannot find any evidence of its use in our configuration, so is **not affected***
- **CVE-2022-30556** – "may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer"
  *I cannot find any evidence of this function's use in SS1200 source, so is **not affected***
- **CVE-2022-31813** – mod_proxy may not send the X-Forwarded-* headers to the origin server
  *SS1200 does not use this module, so is **not affected***

All of these have been fixed in 2.4.54 which the Apache project release on 8-Jun-2022.
The Gentoo project has made this version available, so our next update will be to at least 2.4.54.

CVE-2023-27522 (Apache)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2023-27522
- Refer to Salesforce case **293283** (first reported to us April 2023)

Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55. Special characters in the origin response header can truncate/split the response forwarded to the client.

Severity: High (base score 7.5)

Affected Apache versions 2.4.30 thru 2.4.55

Fix: Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

Products:

2400 SecureSyncs/VersaSyncs

2400 S/S Version	Apache version
1.7.0	
1.6.0	**Still 2.4.54**
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- Refer to Salesforce Case **293283** (first reported to us Feb 2023). Though the report was directed at 1200s, it also applies to 2400s
- Refer to JIRA ticket **CAR-2416**
- **Applicable to** at least versions 1.6.0 and below

1200 SecureSync/9400s:

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

  - Refer to Salesforce Case **293283** (first reported to us April 2023)
  - Refer to JIRA ticket **SSS-1293**
  - **Applicable to** at least versions 5.9.5 and below (as well as the current Beta 5.9.6 release)

- **1232 VelaSyncs: (No longer supported)**
- **NetClock 9300 and 9200 series (No longer supported)**

CVE-2023-25690 (Apache)

- ➢ Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2023-25690
- ➢ Refer to Salesforce case **293283** (first reported to us Feb 2023)

Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning.

Severity: CRITICAL (Base Score 9.8)

Affected Apache versions 2.4.55 and below

Fix: Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.6.0	**Still 2.4.54**
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

  - Refer to Salesforce case **293283** (first reported to us Feb 2023). Though the report was directed at 1200s, it also applies to 2400s
  - Refer to JIRA ticket **CAR-2416**
  - **Applicable to** at least versions 1.6.0 and below

- **1200 SecureSync/9400s:**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- Refer to Salesforce case **293283** (first reported to us Feb 2023)
- Refer to JIRA ticket **SSS-1293**
- **Applicable to** at least versions 5.9.5 and below (as well as the current Beta 5.9.6 release)

- **1232 VelaSyncs: (No longer supported)**
- **NetClock 9300 and 9200 series (No longer supported)**

CVE-2023-0401 (PKCS7 for OpenSSL/HTTPS Certificates)

- Refer to sites such as
- Refer to Salesforce case **293283** (first reported to us Feb 2023)

Description:

Severity: CRITICAL

Products:

- **2400 SecureSyncs/VersaSyncs**
  - Refer to Salesforce case **293283** (first reported to us Feb 2023). Though the report was directed at 1200s, it also applies to 2400s
  - Refer to JIRA ticket **CAR-2416**
  - **Applicable to** at least versions 1.6.0 and below

- **1200 SecureSync/9400s:**
  - Refer to Salesforce case **293283** (first reported to us Feb 2023)
  - Refer to JIRA ticket **SSS-1293**
  - **Applicable to** at least versions 5.9.5 and below (as well as the current Beta 5.9.6 release)

- **1232 VelaSyncs: (No longer supported)**
- **NetClock 9300 and 9200 series (No longer supported)**

CVE-2023-0217 (PKCS7 for OpenSSL/HTTPS Certificates)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2023-0217
- Refer to Salesforce case **293283** (first reported to us Feb 2023)

Description: An invalid pointer dereference on read can be triggered when an application tries to check a malformed DSA public key by the EVP_PKEY_public_check() function. This will most likely lead to an application crash. This function can be called on public keys supplied from untrusted sources which could allow an attacker to cause a denial of service attack. The TLS implementation in OpenSSL does not call this function but applications might call the function if there are additional security requirements imposed by standards such as FIPS 140-3.

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**
- **1200 SecureSync/9400s:**
  - Refer to Salesforce case **293283** (first reported to us Feb 2023)
- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series** No longer supported.

CVE-2023-0286 (x.509 HTTPS certificates)

- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2023-0286
- Refer to Salesforce case **293283** (first reported to us Feb 2023) and **295348** (April 2023)

Description: There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network.

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**
  - Refer to JIRA Ticket **PROJ-277**
- **1200 SecureSync/9400s**
  - Refer to Salesforce case **293283** (first reported to us Feb 2023) and **295348** (April 2023)
  - Dave Lorah posted inquiry to Slack (April 2023)
  - Refer to JIRA Ticket **PROJ-277**
- **1232 VelaSyncs**
- **NetClock 9300 and 9200 series:**

CVE-2023-0217 (PKCS7 for OpenSSL/HTTPS Certificates)

- ➢ Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2023-0217
- ➢ Refer to Salesforce case **293283** (first reported to us Feb 2023)

Description: An invalid pointer dereference on read can be triggered when an application tries to check a malformed DSA public key by the EVP_PKEY_public_check() function. This will most likely lead to an application crash. This function can be called on public keys supplied from untrusted sources which could allow an attacker to cause a denial of service attack. The TLS implementation in OpenSSL does not call this function but applications might call the function if there are additional security requirements imposed by standards such as FIPS 140-3.

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**
- **1200 SecureSync/9400s:**
  - Refer to Salesforce case **293283** (first reported to us Feb 2023)

- ○ **1232 VelaSyncs:**
- ○ **NetClock 9300 and 9200 series** No longer supported.

CVE-2023-0216 (PKCS7 for OpenSSL/HTTPS Certificates)

- ➢ Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2023-0216
- ➢ Refer to Salesforce case **293283** (first reported to us Feb 2023)

Description: An invalid pointer dereference on read can be triggered when an application tries to load malformed PKCS7 data with the d2i_PKCS7(), d2i_PKCS7_bio() or d2i_PKCS7_fp() functions. The result of the dereference is an application crash which could lead to a denial of service attack. The TLS implementation in OpenSSL does not call this function however third party applications might call these functions on untrusted data.

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**
- **1200 SecureSync/9400s:**
  - Refer to Salesforce case **293283** (first reported to us Feb 2023)

- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series No longer supported.**

CVE-2023-0215 (OpenSSL)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2023-0215

Description: The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to support the SMIME, CMS and PKCS7 streaming capabilities, but may also be called directly by end user applications. The function receives a BIO from the caller, prepends a new BIO_f_asn1 filter BIO onto the front of it to form a BIO chain, and then returns the new head of the BIO chain to the caller. Under certain conditions, for example if a CMS recipient public key is invalid, the new filter BIO is freed and the function returns a NULL result indicating a failure. However, in this case, the BIO chain is not properly cleaned up and the BIO passed by the caller still retains internal pointers to the previously freed filter BIO. If the caller then goes on to call BIO_pop() on the BIO then a use-after-free will occur. This will most likely result in a crash. This scenario occurs directly in the internal function B64_write_ASN1() which may cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() on the BIO. This internal function is in turn called by the public API functions PEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream, SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7. Other public API functions that may be impacted by this include i2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream and i2d_PKCS7_bio_stream. The OpenSSL cms and smime command line applications are similarly affected.

Severity: High (7.5)

Affected OpenSSL versions: 1.0.2 to 1.0.2zg,1.1.1 to 1.1.1t, 3.0.0 to 3.0.8

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	OpenSSL version
1.7.0	
1.6.0	Still version 1.1.1q
1.4.3	Updated to version 1.1.1q

  - Refer to JIRA ticket **PROJ-277**

- **1200 SecureSync/9400s:**

1200 S/S Version	OpenSSL version
5.9.6	
5.9.5	OpenSSL still 1.0.2u

  - Refer to Salesforce cases **293283** (first reported to us Feb 2023) and **295348** (April 2023)
  - Refer to JIRA ticket **PROJ-277**
  - Affects versions 5.9.5 and below (expected fix in v5.9.6)

- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series (**No longer supported)

CVE-2022-42889 (Apache)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2022-42889
- Refer to Salesforce cases such as: 289857 and 289630

Description: Apache Commons Text performs variable interpolation, allowing properties to be dynamically evaluated and expanded. The standard format for interpolation is "${prefix:name}", where "prefix" is used to locate an instance of org.apache.commons.text.lookup.StringLookup that performs the interpolation. Starting with version 1.5 and continuing through 1.9, the set of default Lookup instances included interpolators that could result in arbitrary code execution or contact with remote servers. These lookups are: - "script" - execute expressions using the JVM script execution engine (javax.script) - "dns" - resolve dns records - "url" - load values from urls, including from remote servers Applications using the interpolation defaults in the affected versions may be vulnerable to remote code execution or unintentional contact with remote servers if untrusted configuration values are used. Users are recommended to upgrade to Apache Commons Text 1.10.0, which disables the problematic interpolators by default.

Known affected Apache server software versions: Apache HTTP

Severity: CWE-94 (weakness- not a vulnerability)

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1200 SecureSync/9400s (versions x.x.x and below affected)**
  - **Refer to Salesforce Case 289630 (Oct 2022)**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- **1232 VelaSyncs:**
- **Netclock 9300 and 9200 series**:

CVE-2022-37454 (SHA-3)

- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2022-37454
- Refer to Salesforce Case 291350 (Dec 2022)

Description: The Keccak XKCP SHA-3 reference implementation before fdc6fef has an integer overflow and resultant buffer overflow that allows attackers to execute arbitrary code or eliminate expected cryptographic properties. This occurs in the sponge function interface.

Severity

Products:

- **1200/2400 SecureSyncs**
  - **N/A** – doesn't apply. Per Tristan Pensel (with Engineering) 13 Dec 2023 we don't use SHA-3.

QID 150640 (CVE-2022-37436 and CVE-2022-36760)

- Refer to (and excerpted below) https://cve.report/qid/150640

Date Published: 2023-01-31

QID 150640: Apache HTTP Server Prior to 2.4.55 Multiple Security Vulnerabilities

The Apache HTTP Server, colloquially called Apache, is a free and open-source cross-platform web server software.

Affected versions of Apache HTTP Server has multiple vulnerabilities:
CVE-2022-37436 : **mod_proxy** allows a backend to trigger HTTP response splitting
CVE-2022-36760 : **mod_proxy_ajp** possible request smuggling

Affected Versions:
Apache HTTP Server version from 2.4.0 to 2.4.54

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request and checks the response headers to confirm if the host is running vulnerable version of Apache HTTP Server.

Exploitation of the vulnerability could lead to HTTP request splitting or request smuggling attack.

□ **CVSS V3** rated as **Critical** - 9 severity.
□ **CVSS V2** rated as **Medium** - 5 severity.

Solution
Customers are advised to upgrade to the latest version of Apache HTTP Server to remediate this vulnerability. For more information related to this vulnerability please refer to Apache's Security advisory

A) CVE-2022-37436 (Apache: mod_proxy allows a backend to trigger HTTP response splitting)

- ➢ Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2022-37436
- ➢ Refer to Salesforce case **292984** (first reported to us Feb 2023) and JIRA **SSS-1320**

Severity: Medium

Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

Known affected Apache server software versions: Apache **HTTP** Server 2.4 version 2.4.54 and prior versions

(3 Feb 2023 per Ryan Johnson) Hi Keith & Emmanuel -- well I have good news in fact. I brought this up with Will and Tim and these CVEs do not apply to us... The two CVEs apply to the mod_dav, mod_proxy, and mod_proxy_ajp apache modules, none of which are used in either 2400 or 1200 (or Versa) 😳!!!

Products:

- ○ **2400 SecureSyncs/VersaSyncs (Refer to CAR-2238)**

2400 S/S Version	Apache version
1.6.0	**2.4.54**
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- ○ **1232 VelaSyncs:**
- ○ **1200 SecureSync/9400s (Refer to SSS-1320)**

S/S Version	Apache version
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- ○ **NetClock 9300 and 9200 series**:

B) CVE-2022-36760 (Apache: mod_proxy_ajp possible request smuggling)

- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2022-36760
- Refer to Salesforce case **292984** (first reported to us Feb 2023) and JIRA **SSS-1320**

Severity: Critical

Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions

(3 Feb 2023 per Ryan Johnson) Hi Keith & Emmanuel -- well I have good news in fact. I brought this up with Will and Tim and these CVEs do not apply to us... The two CVEs apply to the mod_dav, mod_proxy, and mod_proxy_ajp apache modules, none of which are used in either 2400 or 1200 (or Versa) 😳!!!

Known affected Apache server software versions: Apache **HTTP** Server 2.4 version 2.4.54 and prior versions

Products:

○ **2400 SecureSyncs/VersaSyncs (Refer to CAR-2238)**

2400 S/S Version	Apache version
1.6.0	**2.4.54**
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

○ **1232 VelaSyncs:**

○ **1200 SecureSync/9400s (Refer to SSS-1320)**

S/S Version	Apache version
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

○ **NetClock 9300 and 9200 series**:

CVE-2022-31813 (Apache)

- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2022-31813
- Refer to Salesforce case **267843** (first reported to us July 2022) and JIRA **SSS-1293**

Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

Severity

Known affected Apache server software versions: Apache HTTP Server 2.4.53 and earlier

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.7.0	
1.6.0	**Still 2.4.54**
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1232 VelaSyncs:**
- **1200 SecureSync/9400s (versions 5.9.5 and below affected)**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- **NetClock 9300 and 9200 series**:

CVE-2022-31630 (PHP)

- Refer to: https://nvd.nist.gov/vuln/detail/CVE-2022-31630
- Refer to Salesforce Case 291350 (Dec 2022)

Description In PHP versions prior to 7.4.33, 8.0.25 and 8.2.12, when using imageloadfont() function in gd extension, it is possible to supply a specially crafted font file, such as if the loaded font is used with imagechar() function, the read outside allocated buffer will be used. This can lead to crashes or disclosure of confidential information.

Severity

Affected PHP versions: PHP versions prior to 7.4.33, 8.0.25 and 8.2.12

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	**PHP version**
1.7.0	
1.6.0	Still version 8.0.20
1.4.3	Updated to version 8.0.20
1.4.1	Version 7.4.15
1.2.1 and 1.2.2	Updated to **7.4.4**
1.2.0	? 5.6.35-pl1 ?

- **1200 SecureSync/9400s:**

S/S Version	**PHP version**
5.9.6	
5.9.5	Updated to **7.4.28**
5.9.3/5.9.4	Updated to **7.4.19**
5.9.0	Updated to **7.4.6**
5.8.1	Updated to 5.6.35-pl1

- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series: ?**

CVE-2022-31629 (PHP)

- Refer to sites such https://nvd.nist.gov/vuln/detail/CVE-2022-31629

Description: *In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a `__Host-` or `__Secure-` cookie by PHP applications.*

Affected versions of PHP: PHP versions before 7.4.31, 8.0.24 and 8.1.11

Severity: Medium risk (not critical)

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 **S/S Version**	**PHP version**
1.7.0	
1.6.0	Still version 8.0.20
1.4.3	Updated to version 8.0.20
1.4.1	Version 7.4.15
1.2.1 and 1.2.2	Updated to **7.4.4**
1.2.0	? 5.6.35-pl1 ?

- **1200 SecureSync/9400s:**

S/S Version	**PHP version**
5.9.6	
5.9.5	Updated to **7.4.28**
5.9.3/5.9.4	Updated to **7.4.19**
5.9.0	Updated to **7.4.6**
5.8.1	Updated to 5.6.35-pl1

  - **Refer to Salesforce case 290509 (1st reported to us Nov 2022 in 5.9.5)**

- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series: ?**

CVE-2022-31628 (PHP)

- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2022-31628

Description: *In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompressor code would recursively uncompress "quines" gzip files, resulting in an infinite loop.*

Affected versions of PHP: PHP versions before 7.4.31, 8.0.24 and 8.1.11

Severity: Medium risk (not critical)

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 **S/S Version**	**PHP version**
1.7.0	
1.6.0	Still version 8.0.20
1.4.3	Updated to version 8.0.20
1.4.1	Version 7.4.15
1.2.1 and 1.2.2	Updated to **7.4.4**
1.2.0	? 5.6.35-pl1 ?

- **1200 SecureSync/9400s:**

S/S Version	**PHP version**
5.9.6	
5.9.5	Updated to **7.4.28**
5.9.3/5.9.4	Updated to **7.4.19**
5.9.0	Updated to **7.4.6**
5.8.1	Updated to 5.6.35-pl1

  - **Refer to Salesforce case 290509 (1st reported to us Nov 2022 in 5.9.5)**

- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series: ?**

CVE-2022-31626 (PHP with MySQL)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2022-31626 and

Description: *In PHP versions 7.4.x below 7.4.30, 8.0.x below 8.0.20, and 8.1.x below 8.1.7, **when pdo_mysql extension with mysqlnd driver**, if the third party is allowed to supply host to connect to and the password for the connection, password of excessive length can trigger a buffer overflow in PHP, which can lead to a remote code execution vulnerability.*

Affected versions of PHP: PHP versions 7.4.x below 7.4.30, 8.0.x below 8.0.20, and 8.1.x below 8.1.7

Severity: High

Products:

- **1232 VelaSyncs:**
- **2400 SecureSyncs/VersaSyncs: Not affected. MySQL not installed.**

  Per Ryan Johnson (1 Aug 2022) This CVE does not impact the 1200 (or 2400/Versa) as it is tied to MySQL which is not used in our products.

- **1200 SecureSync/9400s: Not affected. MySQL not installed.**

  Per Ryan Johnson (1 Aug 2022) This CVE does not impact the 1200 (or 2400/Versa) as it is tied to MySQL which is not used in our products.

- **Refer to Salesforce case 263191 (reported July 2022)**
- **NetClock 9300 and 9200 series: ?**

CVE-2022-31625 (PHP)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2022-31625 and https://www.tenable.com/cve/CVE-2022-31625

Description: In PHP versions 7.4.x below 7.4.30, 8.0.x below 8.0.20, and 8.1.x below 8.1.7, when using Postgres database extension, supplying invalid parameters to the parametrized query may lead to PHP attempting to free memory using uninitialized data as pointers. This could lead to RCE vulnerability or denial of service.

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	PHP version
1.7.0	
1.6.0	Still version 8.0.20
1.4.3	Updated to version 8.0.20
1.4.1	Version 7.4.15
1.2.1 and 1.2.2	Updated to **7.4.4**
1.2.0	? 5.6.35-pl1 ?

- **1200 SecureSync/9400s: Doesn't apply. We do not use Postgres database in 1200s**
- **Per Tim Hammer (14 July 2022) This CVE does not apply to SS1200**. We do **not** use Postgres database at all in SS1200. The module is not installed to the unit. No need to create a ticket or escalate further.

S/S Version	PHP version
5.9.6	
5.9.5	Updated to **7.4.28**
5.9.3/5.9.4	Updated to **7.4.19**
5.9.0	Updated to **7.4.6**
5.8.1	Updated to 5.6.35-pl1

- **Refer to Salesforce case** 286734 **(reported July 2022)**
- **Per Tim Hammer (14 July 2022) This CVE does not apply to SS1200**. We ***do not*** use Postgres database at all in SS1200. The module is not installed to the unit. No need to create a ticket or escalate further.

- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series: ?**

CVE-2022-30556 (Apache)

- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2022-30556
- Refer to Salesforce case **267843** (first reported to us July 2022) and JIRA **SSS-1293**

Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

Severity:

Known affected Apache server software versions: Apache HTTP Server 2.4.53 and earlier

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.7.0	
1.6.0	**Still 2.4.54**
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1200 SecureSync/9400s (versions 5.9.5 and below affected)**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series**:

CVE-2022-30522 (Apache)

- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2022-30522
- Refer to Salesforce case **267843** (first reported to us July 2022) and JIRA **SSS-1293**

Description: If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort.

Severity:

Known affected Apache server software versions: Apache HTTP Server 2.4.53

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.7.0	
1.6.0	Still 2.4.54
1.4.3	Updated to 2.4.54
1.4.1	2.4.46
1.4.0	2.4.46
1.2.1 and 1.2.2	2.4.41

- **1232 VelaSyncs:**
- **1200 SecureSync/9400s (at least version 5.9.5 affected)**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- **NetClock 9300 and 9200 series**:

CVE-2022-29404 (Apache)

- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2022-29404
- Refer to Salesforce case **267843** (first reported to us July 2022) and JIRA **SSS-1293**

Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

Severity

Known affected Apache server software versions: Apache HTTP Server 2.4.53 and earlier

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.7.0	
1.6.0	
1.4.3	Updated to 2.4.54
1.4.1	2.4.46
1.4.0	2.4.46
1.2.1 and 1.2.2	2.4.41

- **1200 SecureSync/9400s (versions 5.9.5 and below affected)**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- **1232 VelaSyncs**
- **NetClock 9300 and 9200 series**:

CVE-2022-28614 (Apache)

- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2022-28614
- Refer to Salesforce case **267843** (first reported to us July 2022) and JIRA **SSS-1293**

Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

Severity:

Known affected Apache server software versions: Apache HTTP Server 2.4.53 and earlier

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.7.0	
1.6.0	**Still 2.4.54**
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1232 VelaSyncs:**
- **1200 SecureSync/9400s (versions 5.9.5 and below affected)**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- **NetClock 9300 and 9200 series**:

CVE-2022-28615 (Apache)

- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2022-28615
- Refer to Salesforce case **267843** (first reported to us July 2022) and JIRA **SSS-1293**

Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

Known affected Apache server software versions: Apache HTTP Server 2.4.53 and earlier

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.7.0	
1.6.0	**2.4.54**
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1200 SecureSync/9400s (versions 5.9.5 and below affected)**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- **1232 VelaSyncs:**

- **NetClock 9300 and 9200 series**:

CVE-2022-28330 (Apache in Windows)

- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2022-28330
- Refer to Salesforce case **267843** (first reported to us July 2022) and JIRA **SSS-1293**

Description: on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

Severity:

Known affected Apache server software versions: Apache HTTP Server 2.4.53 and earlier on Windows

Products:

- **2400 SecureSyncs/VersaSyncs (Affects Apache on Windows – SecureSyncs are linux)**
- **1232 VelaSyncs: (Affects Apache on Windows –Velas are linux)**
- **1200 SecureSync/9400s (Affects Apache on Windows – SecureSyncs are linux)**
- **NetClock 9300 and 9200 series**: **(Affects Apache on Windows – NetClocks are linux**

CVE-2022-26377 (Apache)

- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2022-26377
- Refer to Salesforce case **267843** (first reported to us July 2022) and JIRA **SSS-1293**

Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to.

Known affected Apache server software versions: Affects Apache HTTP Server Apache HTTP Server 2.4 version **2.4.53 and prior versions**.

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.6.0	**Still 2.4.54**
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1232 VelaSyncs:**
- **1200 SecureSync/9400s (versions 5.9.5 and below affected)**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- **NetClock 9300 and 9200 series**:

CVE-2022-23812 (package node-ipc)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2022-23812

Description: This affects the package node-ipc from 10.1.1 and before 10.1.3. This package contains malicious code, that targets users with IP located in Russia or Belarus, and overwrites their files with a heart emoji

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**
- **1232 VelaSyncs:**
- **1200 SecureSync/9400s: N/A. Not affected**
  - **Refer to Salesforce case**

    Email from Ron Dries (17 March 2022) I just checked with Engineering quickly and the **node-ipc package is not used in SecureSync 1200. We don't use node.js at all. The SecureSync 1200 should not be impacted**.

NetClock 9300 and 9200 series: ?

CVE-2022-23943 (Apache)

- Refer to sites such as https://cve.mitre.org/cgi-bin/cvename.cgi?name=2022-23943 https://nvd.nist.gov/vuln/detail/CVE-2022-23943
- Refer to Salesforce case 282970 (first reported to us March 2022)

Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data.

Severity:

Known affected Apache server software versions: affects Apache HTTP Server 2.4 version 2.4.52 and prior versions

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.7.0	
1.6.0	Still 2.4.54
1.4.3	Updated to 2.4.54
1.4.1	2.4.46
1.4.0	2.4.46
1.2.1 and 1.2.2	2.4.41

- **1232 VelaSyncs:**
- **1200 SecureSync/9400s** Fixed in 5.9.5 and above **(apparently affects all versions of at least 5.9.4 and below, accept 5.8.1?)**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- **NetClock 9300 and 9200 series**:

CVE-2022-22963 and CVE-2022-22965: Spring Framework vulnerability and Spring4Shell exploit (Spring Framework)

- Refer to sites such as
- Refer to Salesforce case **238186** (first reported to us March 2022)

Description: Spring released emergency updates to fix the 'Spring4Shell' zero-day remote code execution vulnerability, which leaked prematurely online before a patch was released.

What is Spring: Spring is a very powerful yet lightweight Java Enterprise Edition application development framework. There is no need for heavy Java EE application server. Refer to sites such as: https://spring.io/projects/spring-framework

Severity:

Products:

Per Ron Dries (4 April 2022) "I spoke with Engineering and we do not use Java or the Spring framework in SecureSync 1200, 2400, or VersaSync." So we should not be affected"

- **2400 SecureSyncs/VersaSyncs: N/A. See note above from Ron Dries**
- **1200 SecureSync/9400s: N/A. See note above from Ron Dries**
- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series**:

CVE-2022-22721 (Apache)

- ➢ Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2022-22721
- ➢ Refer to Salesforce case 282970 (first reported to us March 2022)

Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

Severity:

Known affected Apache server software versions: affects Apache HTTP Server 2.4.52 and earlier.

Products:

- ○ **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.6.0	**Still 2.4.54**
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- ○ **1232 VelaSyncs:**
- ○ **1200 SecureSync/9400s: Fixed in 5.9.5 and above (apparently affects all versions of at least 5.9.4 and below)**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- ○ **NetClock 9300 and 9200 series**:

CVE-2022-22720 (Apache)

- ➢ Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2022-2272
- ➢ Refer to Salesforce case 282970 (first reported to us March 2022)

Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

Severity:

Known affected Apache server software versions: affects Apache HTTP Server 2.4.52 and earlier.

Products:

- ○ **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.4.3	Updated to 2.4.54
1.4.1	2.4.46
1.4.0	2.4.46
1.2.1 and 1.2.2	2.4.41

- **1232 VelaSyncs:**
- **1200 SecureSync/9400s: Fixed in 5.9.5 and above (apparently affects all versions of at least 5.9.4 and below)**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- **NetClock 9300 and 9200 series**:

CVE-2022-22719 (Apache)

- Refer to sites such as https://cve.mitre.org/cgi-bin/cvename.cgi?name=2022-22719 https://nvd.nist.gov/vuln/detail/CVE-2022-22719
- Refer to Salesforce Case Number 282970 (first reported to us March 2022)

Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash.

Severity:

Known affected Apache server software versions: affects Apache HTTP Server 2.4.52 and earlier.

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.7.0	
1.6.0	Still 2.4.54
1.4.3	Updated to 2.4.54
1.4.1	2.4.46
1.4.0	2.4.46
1.2.1 and 1.2.2	2.4.41

- **1232 VelaSyncs:**
- **1200 SecureSync/9400s: Fixed in 5.9.5 and above (apparently affects all versions of at least 5.9.4 and below)**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- **NetClock 9300 and 9200 series**:

CVE-2022-4450 (OpenSSL/HTTPS Certificates)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2022-4450
- Refer to Salesforce case **293283** (first reported to us Feb 2023)

Description: The function PEM_read_bio_ex() reads a PEM file from a BIO and parses and decodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data. If the function succeeds then the "name_out", "header" and "data" arguments are populated with pointers to buffers containing the relevant decoded data. The caller is responsible for freeing those buffers. It is possible to construct a PEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex() will return a failure code but will populate the header argument with a pointer to a buffer that has already been freed. If the caller also frees this buffer then a double free will occur. This will most likely lead to a crash. This could be exploited by an attacker who has the ability to supply malicious PEM files for parsing to achieve a denial of service attack. The functions PEM_read_bio() and PEM_read() are simple wrappers around PEM_read_bio_ex() and therefore these functions are also directly affected. These functions are also called indirectly by a number of other OpenSSL functions including PEM_X509_INFO_read_bio_ex() and SSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internal uses of these functions are not vulnerable because the caller does not free the header argument if PEM_read_bio_ex() returns a failure code. These locations include the PEM_read_bio_TYPE() functions as well as the decoders introduced in OpenSSL 3.0. The OpenSSL asn1parse command line application is also impacted by this issue.

Severity: High (7.5)

Affected OpenSSL versions (CWE-415: weakness- not a vulnerability)

Products:

- **2400 SecureSyncs/VersaSyncs**
- **1200 SecureSync/9400s:**
  - Refer to Salesforce case **293283** (first reported to us Feb 2023)
- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series No longer supported.**

CVE-2022-4304 ()

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2022-4304
- Refer to Salesforce case **293283** (first reported to us Feb 2023)

Description: A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE. For example, in a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection.

Severity: (CWE: Weakness- not a vulnerability)

Affected versions of OpenSSL

Products:

- **2400 SecureSyncs/VersaSyncs**
- **1200 SecureSync/9400s:**
  - Refer to Salesforce case **293283** (first reported to us Feb 2023)
- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series No longer supported.**

CVE-2022-4203 (x.509 HTTPS certificate)

- Refer to sites such as https://access.redhat.com/security/cve/cve-2022-4203
- Refer to Salesforce case **293283** (first reported to us Feb 2023)

Description: A flaw was found in Open SSL. A read buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification, and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer.

Severity: Moderate/Medium

Affects (CWE-120; weakness- not a vulnerability)

Products:

- **2400 SecureSyncs/VersaSyncs**
- **1200 SecureSync/9400s:**
  - Refer to Salesforce case **293283** (first reported to us Feb 2023)
- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series No longer supported**

CVE-2022-3786 (OpenSSL vulnerability for TLS HTTPS certificates)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2022-3786

Description: A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed a malicious certificate or for an application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address in a certificate to overflow an arbitrary number of bytes containing the `.' character (decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service). In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects.

Severity: High (7.5)

Affects (CWE-120; weakness- not a vulnerability)

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	OpenSSL version
1.7.0	
1.6.0	Still version 1.1.1q
1.4.3	Updated to version 1.1.1q

- **1200 SecureSync/9400s:**

1200 S/S Version	OpenSSL version
5.9.5	OpenSSL still 1.0.2u

  - **Refer to Salesforce Cases such as** 290393
  - Appears this doesn't apply to 1200s, as it's for a newer series of OpenSSL than 1200s have installed

- **1232 VelaSyncs:**

- **NetClock 9300 and 9200 series**:

CVE-2022-3602 (OpenSSL vulnerability for TLS HTTPS certificates)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2022-3602 (x509 certificate buffer overrun)

Description: A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution. Many platforms implement stack overflow protections which would mitigate against the risk of remote code execution. The risk may be further mitigated based on stack layout for any given platform/compiler. Pre-announcements of CVE-2022-3602 described this issue as CRITICAL. Further analysis based on some of the mitigating factors described above have led this to be downgraded to HIGH. Users are still encouraged to upgrade to a new version as soon as possible. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Fixed in OpenSSL 3.0.7 (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6).

Severity:

Affected versions of OpenSSL: **3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6**

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	OpenSSL version
1.7.0	
1.6.0	Still version 1.1.q
1.4.3	Updated to version 1.1.1q

- **1200 SecureSync/9400s:**

1200 S/S Version	OpenSSL version
5.9.6	
5.9.5	OpenSSL still 1.0.2u

  - **Refer to Salesforce Case** 290393
  - Appears this doesn’t apply to 1200s, as it’s for a newer series of OpenSSL than 1200s have installed

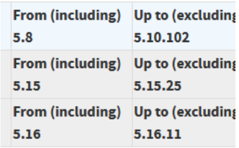
- **1232 VelaSyncs**
- **NetClock 9300 and 9200 series**:

CVE-2022-0847 (Dirty Pipe vulnerability in linux kernels)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2022-0847

Description: A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system.

Associated kernel versions:



From (including) 5.8	Up to (excluding 5.10.102
From (including) 5.15	Up to (excluding 5.15.25
From (including) 5.16	Up to (excluding 5.16.11

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**

  Model 2400 Update version 1.4.1 (April 2022)
  Per 1.4.1 Release Notes: "Applied small patch to kernel to mitigate the Dirty Pipe vulnerability (CVE-2022-0847)"

- **1232 VelaSyncs:**
- **1200 SecureSync/9400s:**
- **NetClock 9300 and 9200 series**:

CVE-2021-44790 (Apache)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2021-44790

Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

Severity:

Known affected Apache server software versions: all versions up to (including) **2.4.5** (Apparently fixed in 2.4.52)

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.6.0	**Still 2.4.54**
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1232 VelaSyncs:**
- **1200 SecureSync/9400s: Fixed in 5.9.5 (and above). Applies to all versions 5.9.4 and below.**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- ○ **Affects ALL Apache versions prior to 2.4.52**. Apache was updated to **2.4.48** in versions 5.9.3/5.9.4.
- ○ **Refer to Salesforce case 277479 and JIRA SSS-1235**

○ **NetClock 9300 and 9200 series**:

CVE-2021-44224 (Apache)

➢ Refer to sites such as https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44224

Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

Severity:

Known affected Apache server software versions: 2.4.7 to 2.4.52

Products:

○ **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.6.0	**Still 2.4.54**
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

○ **1232 VelaSyncs:**

○ **1200 SecureSync/9400s: Fixed in 5.9.5 (and above). Affects all versions 5.9.4 and below.**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- ○ **Affects Apache** versions 2.4.7 to 2.4.52. Apache was updated to **2.4.48** in versions 5.9.3/5.9.4. Then it was updated to **2.4.53** in version **5.9.5.**
- ○ **Refer to Salesforce case 277479 and JIRA SSS-1235**

○ **NetClock 9300 and 9200 series**:

CVE-2021-39275 (Apache)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2021-39275

Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.6.0	**Still 2.4.54**
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1232 VelaSyncs:**
- **1200 SecureSync/9400s: Fixed in 5.9.5 (and above). Affects all versions 5.9.4 and below.**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

  - **Affects Apache** versions 2.4.7 to 2.4.52. Apache was updated to **2.4.48** in versions 5.9.3/5.9.4. Then it was updated to **2.4.53** in version 5.9.5.
  - **Refer to Salesforce case 280456**
- **NetClock 9300 and 9200 series**:

CVE-2021-40438 (Apache Mod_Proxy)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/cve-2021-40438

Description: A crafted request uri-path can cause **mod_proxy** to forward the request to an origin server chosen by the remote user.

Severity:

Affects: This issue affects Apache HTTP Server 2.4.48 and earlier.

Products:

- **2400 SecureSyncs/VersaSyncs**
  - Note Per Ryan Johnson: "We do not use the mod_proxy or mod_proxy_uwsgi modules in SS2400/Versa and therefore do not impact us"

- **1200 SecureSync/9400s: Fixed in 5.9.5 (and above). Affects all versions 5.9.4 and below.**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

  - **Affects Apache** versions 2.4.7 to 2.4.52. Apache was updated to **2.4.48** in versions 5.9.3/5.9.4. Then it was updated to **2.4.53** in version **5.9.5.**
  - **Refer to Salesforce case 277479 and JIRA SSS-1235**

- **1232 VelaSyncs:**

- **NetClock 9300 and 9200 series:**

CVE-2021-36160 (Apache)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2021-36160

Description: A carefully crafted request uri-path can cause **mod_proxy_uwsgi** to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.4.3	Updated to 2.4.54
1.4.1	2.4.46
1.4.0	2.4.46
1.2.1 and 1.2.2	2.4.41

- **1200 SecureSync/9400s: Fixed in 5.9.5 (and above). Affects all versions 5.9.4 and below.**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

  - **Affects Apache** versions 2.4.7 to 2.4.52. Apache was updated to **2.4.48** in versions 5.9.3/5.9.4. Then it was updated to **2.4.53** in version **5.9.5.**
  - **Refer to Salesforce case 277479 and JIRA SSS-1235**

- **1232 VelaSyncs:**

- **NetClock 9300 and 9200 series:**

CVE-2021-34798 (Apache)

Description: Malformed requests may cause the server to dereference a NULL pointer.

Severity:

Affects: This issue affects Apache **HTTP Server 2.4.48** and earlier

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.6.0	**Still 2.4.54**
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1200 SecureSync/9400s: Fixed in 5.9.5 (and above). Affects all versions 5.9.4 and below.**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

  - **Affects Apache** versions 2.4.7 to 2.4.52. Apache was updated to **2.4.48** in versions 5.9.3/5.9.4. Then it was updated to **2.4.53** in version **5.9.5.**
  - Refer to Salesforce Case 280456

- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series:**

CVE-2021-30641 (Apache)

➢ This CVE is reported as being part of the Apache version 2.4.47 changelog

Description:

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	**Apache version**
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1232 VelaSyncs:**
- **1200 SecureSync/9400s: (affects v5.9.3 and below)**

S/S Version	**Apache version**
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

  - Refer to Salesforce Case 281482
  - I recommended upgrade to v5.9.4, which updates Apache to version 2.4.48.
- **NetClock 9300 and 9200 series**:

CVE-2021-27108 (PHP)

- Refer to sites such as: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27108

Description:

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	PHP version
1.7.0	
1.6.0	Still 8.0.20
1.4.3	Updated to version 8.0.20
1.4.1	Version 7.4.15
1.2.1 and 1.2.2	Updated to **7.4.4**
1.2.0	? 5.6.35-pl1 ?

- **1232 VelaSyncs:**
- **1200 SecureSync/9400s: Fixed in 5.9.5 (and above). Affects all versions 5.9.4 and below.**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

  - **Affects Apache** versions 2.4.7 to 2.4.52. Apache was updated to **2.4.48** in versions 5.9.3/5.9.4. Then it was updated to **2.4.53** in version **5.9.5.**

- **NetClock 9300 and 9200 series**:

CVE-2021-27105 (PHP)

- Refer to sites such as: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-27105

Description: In **PHP** versions 7.3.x below 7.3.29, **7.4.x below 7.4.21** and 8.0.x below 8.0.8, when using URL validation functionality via filter_var() function **with FILTER_VALIDATE_URL parameter**, an URL with invalid password field can be accepted as valid. This can lead to the code incorrectly parsing the URL and potentially leading to other security implications - like contacting a wrong server or making a wrong access decision.

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	PHP version
1.6.0	Still 8.0.20
1.4.3	Updated to version 8.0.20
1.4.1	Version 7.4.15
1.2.1 and 1.2.2	Updated to **7.4.4**
1.2.0	? 5.6.35-pl1 ?

- **1232 VelaSyncs:**
- **1200 SecureSync/9400s:**
  - **Refer to Salesforce case 283648 (reported April 2022)**
  - **PHP version updated to 7.4.28 in version 5.9.5 (July 2022)**

S/S Version	PHP version
5.9.6	
5.9.5	Updated to **7.4.28**
5.9.3/5.9.4	Updated to **7.4.19**
5.9.0	Updated to **7.4.6**
5.8.1	Updated to 5.6.35-pl1

- **NetClock 9300 and 9200 series**:

CVE-2021-27104 (PHP **when using Firebird PDO driver extension**)

- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2021-27104

Description: In PHP versions **7.3.x below 7.3.29, 7.4.x below 7.4.21 and 8.0.x below 8.0.8**, **when using Firebird PDO driver extension,** a malicious database server could cause crashes in various database functions, such as getAttribute(), execute(), fetch() and others by returning invalid response data that is not parsed correctly by the driver. This can result in crashes, denial of service or potentially memory corruption.

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**
- **1200 SecureSync/9400s:**
    - **Refer to Salesforce case 283648 (reported April 2022)**
    - I suspect we do not use “Firebird PDO driver” in our products. So this is likely N/A. Need to confirm with Engineering though.
- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series:**

CVE-2021-27103 (PHP with Accellion)

- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2021-27103

Description: Accellion FTA (https://www.accellion.com/products/fta/) 9_12_411 and earlier is affected by SSRF via a crafted POST request to wmProgressstat.html. The fixed version is FTA_9_12_416 and later.

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**
- **1200 SecureSync/9400s:**
    - **Refer to Salesforce case 277479)**
    - **I suspect we do not use Accellion in our products and so this is N/A. Need to confirm this with Engineering.**
- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series:**

CVE-2021-26691 (Apache)

- This CVE is reported as being part of the Apache version 2.4.47 changelog

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	*Apache version*
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1200 SecureSync/9400s: (affects v5.9.3 and below)**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

  - Refer to Salesforce Case 281482
  - I recommended upgrade to v5.9.4, which updates Apache to version 2.4.48.

- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series:**

CVE-2021-26690 (Apache)

- This CVE is reported as being part of the Apache version 2.4.47 changelog

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.4.3	Updated to 2.4.54
1.4.1	2.4.46
1.4.0	2.4.46
1.2.1 and 1.2.2	2.4.41

- **1200 SecureSync/9400s: (affects v5.9.3 and below)**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

  - Refer to Salesforce Case 281482
  - This CVE is reported as being part of the Apache version 2.4.47 changelog
  - I recommended upgrade to at least v5.9.4, which updated Apache to version 2.4.48.

- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series:**

CVE-2021-21704 and CVE-2021-21705 (PHP v7.4.6)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2021-21704

CVE 21704: In PHP versions 7.3.x below 7.3.29, **7.4.x below 7.4.21** and 8.0.x below 8.0.8, when using Firebird PDO driver extension, a malicious database server could cause crashes in various database functions, such as getAttribute(), execute(), fetch() and others by returning invalid response data that is not parsed correctly by the driver. This can result in crashes, denial of service or potentially memory corruption.

CVE 21705: In PHP versions 7.3.x below 7.3.29, 7.4.x below 7.4.21 and 8.0.x below 8.0.8, when using URL validation functionality via filter_var() function with FILTER_VALIDATE_URL parameter, an URL with invalid password field can be accepted as valid. This can lead to the code incorrectly parsing the URL and potentially leading to other security implications - like contacting a wrong server or making a wrong access decision.

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	PHP version
1.6.0	Still 8.0.20
1.4.3	Updated to 8.0.20
1.4.1	Version 7.4.15
1.2.1 and 1.2.2	Updated to **7.4.4**
1.2.0	? 5.6.35-pl1 ?

- **1200 SecureSync/9400s: (Not applicable to 1200 SecureSyncs)**
  - Refer to Salesforce Case 276981

S/S Version	PHP version	Comments
5.9.6		
5.9.5	Updated to 7.4.28	PHP updated to 7.4.28. Version now out of associated range
5.9.3/5.9.4	Updated to 7.4.19	Not affected. See email below
5.9.0	Updated to 7.4.6	Not affected. See email below
5.8.1	Updated to 5.6.35-pl1	Not affected. See email below

  - **Email from Tim Hammer to Dave Lorah (16 Dec 2021)** "I have confirmed that SS1200 does not contain any modules or code that is impacted by these two CVEs:

    * CVE-2021-21704
    * CVE-2021-21705

- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series:**

CVE-2021-21708 (PHP “php_filter_float function”)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2021-21708

Description: In PHP versions 7.4.x below 7.4.28, 8.0.x below 8.0.16, and 8.1.x below 8.1.3, when using filter functions with FILTER_VALIDATE_FLOAT filter and min/max limits, if the filter fails, there is a possibility to trigger use of allocated memory after free, which can result it crashes, and potentially in overwrite of other memory chunks and RCE. This issue affects: code that uses FILTER_VALIDATE_FLOAT with min/max limit

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 **S/S Version**	**PHP version**
1.4.3	Updated to version 8.0.20
1.4.1	Version 7.4.15
1.2.1 and 1.2.2	Updated to **7.4.4**
1.2.0	? 5.6.35-pl1 ?

- **1232 VelaSyncs:**
- **1200 SecureSync/9400s: (per Tim hammer, does not appear it affects 1200 SecureSyncs. See his email further below)**
  - **Refer to Salesforce cases 282970 and 282015 (reported March 2022)**

S/S Version	**PHP version**	**Comments**
5.9.6		
5.9.5	Updated to 7.4.28	PHP updated to 7.4.28. Version now out of associated range
5.9.3/5.9.4	Updated to 7.4.19	Not affected. See email below
5.9.0	Updated to 7.4.6	Not affected. See email below
5.8.1	Updated to 5.6.35-pl1	Not affected. See email below

Email from Jodi to customer (based on report from Tim hammer) Our Engineering Team looked into this vulnerability. For the SecureSync device, **we found no usage of the php_filter_float function**.

In regards to the vulnerability CVE-2021-21708: "In PHP versions 7.4.x below 7.4.28, 8.0.x below 8.0.16, and 8.1.x below 8.1.3, when using filter functions with FILTER_VALIDATE_FLOAT filter and min/max limits, if the filter fails, there is a possibility to trigger use of allocated memory after free, which can result it crashes, and potentially in overwrite of other memory chunks and RCE. **This issue affects: code that uses FILTER_VALIDATE_FLOAT with min/max limits."** (from cve.mitre.org, emphasis added).

In short, it does not appear that our SecureSync/Netclock devices are affected by this particular vulnerability.

- **NetClock 9300 and 9200 series**:

CVE-2021-21707 (PHP)

- Refer to sites such as https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21707

Description: In PHP versions 7.3.x below 7.3.33**, 7.4.x below 7.4.26** and 8.0.x below 8.0.13, certain XML parsing functions, like simplexml_load_file(), URL-decode the filename passed to them. If that filename contains URL-encoded NUL character, this may cause the function to interpret this as the end of the filename, thus interpreting the filename differently from what the user intended, which may lead it to reading a different file than intended.

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 **S/S Version**	**PHP version**
1.4.3	Updated to version 8.0.20
1.4.1	Version 7.4.15
1.2.1 and 1.2.2	Updated to **7.4.4**
1.2.0	? 5.6.35-pl1 ?

- **1232 VelaSyncs:**
- **1200 SecureSync/9400s: (apparently affects at least v5.9.3 and below)**
  - **Refer to Salesforce case 274646. Detected in a customer's scan after updating to 5.9.3**

S/S Version	**PHP version**	**Comments**
5.9.6		
5.9.5	Updated to 7.4.28	PHP updated to 7.4.28. Version now out of associated range
5.9.3/5.9.4	Updated to 7.4.19	Not affected. See email below
5.9.0	Updated to 7.4.6	Not affected. See email below
5.8.1	Updated to 5.6.35-pl1	Not affected. See email below

Email from Tim Hammer 2 Dec 2021 Keith has confirmed that the CVE reported by the customer is actually CVE-2021-21707 (and not 21703).

This one does affect SS1200 as it is in "general use" functionality, and I have identified instances of the functionality being used in our PHP code.

Those instances are mostly in the CakePHP library files, but some in our app files as well.

I have looked at the two (2) instances in our application files and am confident that the only possibility of encountering the issue is if some installs a Locale (language.xml) file *in a path that includes the URL-encoded NUL character*.

There are too many instances of the functionality in the CakePHP library files for me to do a reasonable check of if there is a risk of encountering the issue.

The NVD CVSS Version 3.x severity score is 5.3 (medium) and from my understanding of the issue, the result of encountering a URL-encoded NUL character in a path/file name is that the wrong file would be read. If a user has the capability to provide the path/file to be read, and that somehow allows them to access a file they should not have access to, they can access the file without the NUL character in the path/file string they provide and there is no reason to try and circumvent anything with the NUL character.

(But I make no claims to being a security expert and have never been able to think like a "black hat" (or even a "white hat"), so I could very well be missing the crux of the problem…)

- **NetClock 9300 and 9200 series**:

CVE-2021-21703 (PHP)

- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2021-21703 and https://access.redhat.com/security/cve/cve-2021-21703

Per https://nvd.nist.gov/vuln/detail/CVE-2021-21703

Description: *"In PHP versions 7.3.x up to and including 7.3.31,* ***7.4.x below 7.4.25*** *and 8.0.x below 8.0.12*, when running PHP FPM SAPI with main FPM daemon process running as root and child worker processes running as lower-privileged users, *it is possible for the child processes to access memory shared with the main process and write to it, modifying it in a way that would cause the root process to conduct invalid memory reads and writes, which can be used to escalate privileges from local unprivileged user to the root user."*

Per https://access.redhat.com/security/cve/cve-2021-21703

Description*:* *php-fpm has a vulnerability which may lead to local privilege escalation.* **This vulnerability is hard to exploit as the attack needs to escape the FPM sandbox mechanism.** *When a complete attack is achieved it may lead to risk for confidentiality, data integrity, and system availability.*

Statement*:* *This vulnerability affects only systems with php-fpm enabled on its configuration. For an attack to be completed successfully, the attacker needs to chain this vulnerability with some other vulnerability that allows escape from the FPM sandbox first.*

Severity:

Affects This vulnerability affects only systems with php-fpm enabled on its configuration.

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	PHP version
1.7.0	
1.6.0	Still 8.0.20
1.4.3	Updated to version 8.0.20
1.4.1	Version 7.4.15
1.2.1 and 1.2.2	Updated to **7.4.4**
1.2.0	? 5.6.35-pl1 ?

- **1200 SecureSync/9400s: (apparently affects 5.9.4 and below. Fix is in v5.9.5)**

S/S Version	PHP version
5.9.6	
5.9.5	Updated to **7.4.28**
5.9.3/5.9.4	Updated to **7.4.19**
5.9.0	Updated to **7.4.6**
5.8.1	Updated to 5.6.35-pl1

  - Refer to Salesforce case 274646. Detected in customer's 5.9.1 scan. But not detected after updating to v5.9.3

- **1232 VelaSyncs**

- **NetClock 9300 and 9200 series:**

CVE-2021-21702 (PHP)

➢ Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2021-21702

Description: when using SOAP extension to connect to a SOAP server, a malicious SOAP server could return malformed XML data as a response that would cause PHP to access a null pointer and thus cause a crash.

Severity:

Affect PHP versions 7.3.x below 7.3.27, 7.4.x below 7.4.15 and 8.0.x below 8.0.2

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	PHP version
1.4.3	Updated to version 8.0.20
1.4.1	Version 7.4.15
1.2.1 and 1.2.2	Updated to **7.4.4**
1.2.0	? 5.6.35-pl1 ?

- **1200 SecureSync/9400s:**
    - **Refer to Salesforce case 278337.**

S/S Version	PHP version
5.9.6	
5.9.5	Updated to **7.4.28**
5.9.3/5.9.4	Updated to **7.4.19**
5.9.0	Updated to **7.4.6**
5.8.1	Updated to 5.6.35-pl1

- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series:**

CVE-2021-4034 (Polkit linux vulnerability)

Refer to: https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034

https://www.zdnet.com/article/major-linux-policykit-security-vulnerability-uncovered-pwnkit/

Email from Ryan Johnson (27 Jan 2022) I wanted to give you a heads up on a Linux vulnerability that is hitting the news so you can be prepared if/when customer questions come in. This vulnerability, CVE-2021-4034, impacts a Linux daemon named “Polkit” (formerly known as PolicyKit).

https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034

https://www.zdnet.com/article/major-linux-policykit-security-vulnerability-uncovered-pwnkit/

Nicolas has provided this information regarding impact on our products:

*Since it relies on a bug in the polkit software, the following products are **not** affected since they don't include it:*

- *SecureSync 2400*
- *VersaSync*
- *graphene (GUIDE, Gecko, StarSync, or whatever the name ^^')*
- *4 in 1 option cards (1204-4A, 1204-49, 1204-51, 1204-4E)*
- *SecureSync 1200*

*On the contrary, the VelaSync product **may** be affected (read: it's highly probable), since it seems to be using polkit.*

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**
  - *Since it relies on a bug in the polkit software,* SecureSync 2400s/VersaSyncs are not affected
- **1200 SecureSync/9400s:**
  - Since it relies on a bug in the polkit software, SecureSync 1200 is not affected
- **1232 VelaSyncs:**
  - On the contrary, the VelaSync product **may** be affected (read: it's highly probable), since it seems to be using polkit.
- **NetClock 9300 and 9200 series:**

CVE-2021-3156 CVE-2021-23239 CVE-2021-23240 (Sudo vulnerabilities)

- **Refer to**: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3156 https://access.redhat.com/security/cve/cve-2021-3156

Description: Sudo before 1.9.5p2 contains an off-by-one error that can result in a heap-based buffer overflow, which allows privilege escalation to root via "sudoedit -s" and a command-line argument that ends with a single backslash character.

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**
- **1200 SecureSync/9400s:**
  - Versions 5.9.2 and below are susceptable
  - **Fixed in v5.9.3** with sudo package update

    Per Tim Hammer (27 Sept 2021) In 5.9.3 the sudo package was updated to **1.9.6p1** to address several CVEs, including CVE-2021-3156. The work was completed under SSS-1170 which is a sub-task under the general 5.9.3 release creation ticket SSS-1165.
- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series:**

CVE-2020-11896/CVE-2020-11897/CVE-2020-11898/CVE-2020-11899) “Ripple20”

- group of TCP/IP related vulnerabilities (associated with the “**Treck**” package)
- Refer to sites such as: https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come/ (Except further below):

Severity:

Products:

- **2400 SecureSyncs**

2400 S/S Version	Apache version
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1200 SecureSync/9400s: ?**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- **1232 Velasyncs**
- **Legacy VelaSync: ?**
- **NetClock 9300 and 9200 series: ?**

In a security advisory that will go live today and reviewed by ZDNet under embargo, the US Department of Homeland Security has attributed ratings of 10 and 9.8 on the CVSSv3 vulnerability severity scale (scale goes from 1 to 10) to four of the Ripple 20 vulnerabilities. These are:

- **CVE-2020-11896** - CVSSv3 score: 10 - Improper handling of length parameter inconsistency in IPv4/UDP component when handling a packet sent by an unauthorized network attacker. This vulnerability may result in remote code execution.
- **CVE-2020-11897** - CVSSv3 score: 10 - Improper handling of length parameter inconsistency in IPv6 component when handling a packet sent by an unauthorized network attacker. This vulnerability may result in possible out-of-bounds write.
- **CVE-2020-11898** - CVSSv3 score: 9.8 - Improper handling of length parameter inconsistency in IPv4/ICMPv4 component when handling a packet sent by an unauthorized network attacker. This vulnerability may result in exposure of sensitive information.
- **CVE-2020-11899** - CVSSv3 score: 9.8 - Improper input validation in IPv6 component when handling a packet sent by an unauthorized network attacker. This vulnerability may allow exposure of sensitive information.

These four vulnerabilities, when weaponized, could allow attackers to easily take over smart devices or any industrial or healthcare equipment. Attacks are possible via the internet if the devices are connected online, or from local networks if the attacker gains a foothold on an internal network (for example, via a compromised router).

CVE-2020-13938 (Apache)

- This CVE is reported as being part of the Apache version 2.4.47 changelog

Severity:

Affected versions of Apache: Apache version 2.4.47

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1200 SecureSync/9400s: (affects v5.9.2 and below)**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

  - Refer to Salesforce Case 281482
  - I recommended upgrade to v5.9.4, which updates Apache to version 2.4.48.

- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series:**

CVE-2020-11993 (Apache browser vulnerability)

- **Refer to**: https://nvd.nist.gov/vuln/detail/CVE-2020-11993

Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

Severity:

Affects: Apache HTTP Server versions **2.4.20 to 2.4.43**

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1200 SecureSync/9400s:**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

  - Reported by customer in v5.9.0 security scan
  - Refer to**:** SF Case 256640 /JIRA SSS-1098
  - Apparently affects versions 5.9.2 and below

- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series:**

CVE-2020-11984 (Apache mod_proxy)

- **Refer to**: https://nvd.nist.gov/vuln/detail/CVE-2020-11984

Description: Apache HTTP server 2.4.32 to 2.4.44 **mod_proxy_uwsgi** info disclosure and possible RCE

Severity:

Products:

- **2400 Securesyncs/VersaSyncs**

2400 S/S Version	Apache version
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1200 SecureSync/9400s:**

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

  - Reported by customer in v5.9.0 security scan
  - Refer to**:** Salesforce Case 256640 /JIRA SSS-1098

- **1232 VelaSync**
- **NetClock 9300 and 9200 series:**

CVE-2020-9490 (Apache browser vulnerability)

- **Refer to**: https://nvd.nist.gov/vuln/detail/CVE-2020-9490
- **Description**: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers

Severity:

Affects Apache: versions 2.4.20 to 2.4.43

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.4.3	**Updated to 2.4.54**
1.4.1	**2.4.46**
1.4.0	**2.4.46**
1.2.1 and 1.2.2	**2.4.41**

- **1200 SecureSync/9400s:**
  - Reported by customer in v5.9.0 security scan
  - Refer to**:** Salesforce Case 256640 /JIRA SSS-1098
- **1232 VelaSyncs**
- **NetClock 9300 and 9200 series:**

CVE-2020-7068 (PHP - Use-After-Free Issue)

- **Description**: In PHP versions 7.2.x below 7.2.33, 7.3.x below 7.3.21 and **7.4.x below 7.4.9**, while processing PHAR files using phar extension, phar_parse_zipfile could be tricked into accessing freed memory, which could lead to a crash or information disclosure.
- **Refer to**: https://nvd.nist.gov/vuln/detail/CVE-2020-7068
- Discovered in v5.9.1
- Refer to Salesforce Case **258597** and JIRA **SSS-1125**.

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 **S/S Version**	**PHP version**
1.4.3	Updated to version 8.0.20
1.4.1	Version 7.4.15
1.2.1 and 1.2.2	Updated to **7.4.4**
1.2.0	? 5.6.35-pl1 ?

- **1200 SecureSync/9400s: applicable to at least versions 5.9.0/5.9.1 (not applicable to versions 5.8.9 and below)**

S/S Version	**PHP version**
5.9.6	
5.9.5	Updated to 7.4.28
5.9.3/5.9.4	Updated to 7.4.19
5.9.0	Updated to 7.4.6
5.8.1	Updated to 5.6.35-pl1

  - First reported after update to 5.9.1 (March 2021).
  - PHP updated from versions 5.5.38-p10 to 7.4.6 in v5.9.0/5.9.1

CVE-2020-1967 (OpenSSL vulnerability)

- **Refer to**:
- **Description**:

Severity:

Affects

Products:

- **VersaSyncs**
- **1200 SecureSync/9400s:**

    - OpenSSL was updated to 1.0.2u in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series:**
    - OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers

----

CVE-2000-1967 (overflow bug in the x64_64 Montgomery squaring procedure)

- ➢ refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2019-1551

Description: There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible.

Severity:

Products:

- **VersaSyncs:**
- **1200 SecureSync/9400s:**
    - **Per the v5.9.0 update release notes: "**OpenSSL version 1.0.2u has a few known CVE security vulnerabilities (CVE-2019-1551, CVE-2000-1967).
- **1232 VelaSyncs**:
- **Legacy 1225 VelaSync:**
- **NetClock 9300 and 9200 series:**

CVE-2019-18218 (file -- security update)

- ➢ Refer to

Severity:

Products:

- ○ **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- ○ **Legacy VelaSync: ?**
- ○ **1200 SecureSync/9400s:** ?
- ○ **NetClock 9300 and 9200 series**: ?

CVE-2019-17567 (Apache)

- ➢ This CVE is reported as being part of the Apache version 2.4.47 changelog

Affected version: Apache version 2.4.47

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	Apache version
1.4.3	Updated to 2.4.54
1.4.1	2.4.46
1.4.0	2.4.46
1.2.1 and 1.2.2	2.4.41

- **1200 SecureSync/9400s: (affects v5.9.3 and below)**
  - Refer to Salesforce Case 281482
  - I recommended upgrade to v5.9.4, which updates Apache to version 2.4.48.
- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series:**

CVE-2019-15296 (Debian linux, linux-4.9 -- security update)

- Refer to

Severity:

Products:

- **2400 SecureSyncs**
- **1200 SecureSync/9400s: ?**
- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **NetClock 9300 and 9200 series: ?**

CVE-2019-15292 (Debian linux, linux-4.9 -- security update)

- Refer to

Severity

Products:

- **2400 SecureSyncs**
- **1200 SecureSync/9400s: ?**
- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **NetClock 9300 and 9200 series: ?**

CVE-2019-15166 (tcpdump -- security update)

- ➢ Refer to

Products:

- **2400 SecureSyncs**
- **1200 SecureSync/9400s: ?**
- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**

- **NetClock 9300 and 9200 series: ?**

CVE-2019-16227 (tcpdump -- security update)

- ➢ Refer to

Products:

- **1200 SecureSync/9400s: ?**
- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **NetClock 9300 and 9200 series: ?**

CVE-2019-14287 (sudo -- security update)

- ➢ Refer to

Products:

- **1200 SecureSync/9400s: ?**
- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **NetClock 9300 and 9200 series: ?**

CVE-2019-12735 (neovim, vim -- security update)

- ➢ Refer to

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s: ?**

- **NetClock 9300 and 9200 series: ?**

CVE-2019-11815 (Debian linux, linux-4.9 -- security update)

- Refer to

Products:

- **1200 SecureSync/9400s: ?**
- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **NetClock 9300 and 9200 series: ?**

CVE-2019-11043 (php5, php7.0, php7.3 -- security update)

- Refer to

Severity:

Affected versions of PHP:

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	PHP version
1.4.3	Updated to 8.0.20
1.4.1	7.4.15
1.2.1 and 1.2.2	Updated to **7.4.4**
1.2.0	? 5.6.35-pl1 ?

- **1200 SecureSync/9400s:**
  - PHP was updated to 7.4.6 in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)

S/S Version	PHP version
5.9.6	
5.9.5	Updated to 7.4.28
5.9.3/5.9.4	Updated to 7.4.19
5.9.0	Updated to 7.4.6
5.8.1	Updated to **5.6.35-pl1**

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0**
- **Legacy VelaSync: ?**
- **NetClock 9300 and 9200 series: ?**

CVE-2019-10126 (linux, linux-4.9 -- security update)

- Refer to

Severity:

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2019-10098 / CVE-2019-10097 / CVE-2019-10092 / CVE-2019-10082 / CVE-2019-10081

- **Refer to**:
- **Description**: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL
- **Severity:**

Products:

- **2400 SecureSyncs/VersaSyncs**
- **1200 SecureSync/9400s:**
  - Apache was updated to 2.4.41 in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **1232 VelaSyncs:**
  - Refer to Salesforce Case 286821.
  - Velasync v1.2.2 has Apache v2.4.25 installed. “The CVE-2019-10098 is not applicable to the Model Velasync 1232.”
- **NetClock 9300 and 9200 series: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.**

CVE-2019-9517

- **Refer to**:
- **Description**:

Severity:

Products:

- **1200 SecureSync/9400s:**

- Apache was updated to 2.4.41 in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)

- **VersaSyncs**
- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series:**
  - OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers

----

CVE 2019-6111, CVE 2019-6110, CVE 2019-6109 (OpenSSH)

- ➢ Refer to
- ➢ Need to upgrade to OpenSSH version 8.1

Severity:

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** OpenSSH was updated to 8.1p1 in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **NetClock 9300 and 9200 series**: ?

CVE-2019-3846: linux, linux-4.9 -- security update

- ➢ Refer to

Severity:

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2019-1563 (OpenSSL vulnerability)

- ➢ **Refer to**:
- ➢ **Description**:

Severity:

Products:

- **VersaSyncs**
- **1200 SecureSync/9400s:**

  - OpenSSL was updated to **1.0.2u in v5.9.0** update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series:**
  - OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.

CVE-2019-1559 (OpenSSL vulnerability)

- **Refer to**:
- **Description**:

Severity:

Products:

- **1200 SecureSync/9400s:**
  - OpenSSL was updated to 1.0.2u in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **VersaSyncs**
- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series:**
  - OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.

CVE-2019-1551 (overflow bug in the x64_64 Montgomery squaring procedure)

- refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2019-1551

Severity:

Description: There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible.

Products:

- **1232 VelaSyncs:**
- **Legacy 1225 VelaSync:**
- **VersaSyncs:**
- **1200 SecureSync/9400s:**
  - **Per the v5.9.0 update release notes: "**OpenSSL version 1.0.2u has a few known CVE security vulnerabilities (CVE-2019-1551, CVE-2000-1967)."
- **NetClock 9300 and 9200 series**:

CVE-2019-1551 (OpenSSL vulnerability)

- **Refer to**:
- **Description**:

Products:

- **VersaSyncs**
- **1232 VelaSyncs:**
- **1200 SecureSync/9400s:** OpenSSL was updated to 1.0.2u in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.

CVE-2019-1547 (OpenSSL vulnerability)

- **Refer to**:
- **Description**:

Products:

- **VersaSyncs**
- **1232 VelaSyncs:**

- **1200 SecureSync/9400s:** OpenSSL was updated to 1.0.2u in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.

CVE-2019-0211 (RAMBleed Attack Allows Attackers to Read Secret Key Bits)

- ➢ refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2019-0174 https://sensorstechforum.com/cve-2019-0174-rambleed/ https://www.cvedetails.com/cve/CVE-2019-0174/
- ➢ First reported to us on 5 Nov 2019 (refer to case 214294)
- ➢ associated **only** with several **INTEL** processors (listed at https://www.cvedetails.com/cve/CVE-2019-0174/)

Description: Logic condition in specific microprocessors may allow an authenticated user to potentially enable partial physical address information disclosure via local access.

Products: ***confirming with Apps team, 5 Nov 2019)***

- **1232 VelaSyncs:** N/A- This is a **Supermicro** device so shouldn't be impacted??
- **Legacy 1225 VelaSync:** N/A- This is a Supermicro device so shouldn't be impacted??
- **VersaSyncs:**
- **1200 SecureSync/9400s:**
- **NetClock 9300 and 9200 series**:

CVE-2019-0211: (Apache 2.4.17 to 2.4.38)

- ➢ Refer to sites such as**:** https://nvd.nist.gov/vuln/detail/CVE-2019-0211
- ➢ First reported to us on 20 May (refer to case 195542)

Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

Severity:

Products:

- **1232 VelaSyncs:** Versions 1.1.1 and v1.1.0 are Apache 2.4.25??? (So at least versions 1.1.1 and 1.1.0 are susceptible)
- **VersaSyncs:**
- **1200 SecureSync/9400s:** Apache was updated to 2.4.41 in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **NetClock 9300 and 9200 series**:
- **Legacy 1225 VelaSync: ?**

CVE-2019-0190

- **Refer to**:
- **Description**:

Severity:

Products:

- **VersaSyncs**
- **1232 VelaSyncs:**
- **1200 SecureSync/9400s:** Apache was updated to 2.4.41 in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.

CVE-2018-20836: linux, linux-4.9 -- security update

- Refer to

Severity:

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2018-17199 / CVE-2018-17190 / CVE-2018-17189

- ➢ **Refer to**:
- ➢ **Description**:

Severity:

Products:

- **2400 SecureSyncs**
- **1200 SecureSync/9400s:**

1200 S/S Version	PHP version
5.9.6	
5.9.5	Updated to **7**
5.9.3/5.9.4	Updated to **7.4.19**
5.9.0	Updated to **7.4.6**
5.8.1	Updated to 5.6.35-pl1

  - Apache was updated to 2.4.41 in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)

- **VersaSyncs**
- **1232 VelaSyncs:**
- **NetClock 9300 and 9200 series:**
  - OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.

CVE-2018-17082 (PHP vulnerability)

- ➢ **Refer to**: https://nvd.nist.gov/vuln/detail/CVE-2018-17082

- ➢ **Description**: The Apache2 component in PHP before 5.6.38, 7.0.x before 7.0.32, 7.1.x before 7.1.22, and 7.2.x before 7.2.10 allows XSS via the body of a "Transfer-Encoding: chunked" request, because the bucket brigade is mishandled in the php_handler function in sapi/apache2handler/sapi_apache2.c.

Severity:

Affected versions of PHP: PHP before 5.6.38, 7.0.x before 7.0.32, 7.1.x before 7.1.22, and 7.2.x before 7.2.10

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	PHP version
1.6.0	Still version 8.0.20
1.4.3	Updated to version 8.0.20
1.4.1	Version 7.4.15
1.2.1 and 1.2.2	Updated to **7.4.4**
1.2.0	? 5.6.35-pl1 ?

- **1200 SecureSync/9400s:**
  - PHP was updated to 7.4.6 in **v5.9.0 update**, resolving this vulnerability (refer to v5.9.0 Release Notes)

1200 S/S Version	PHP version
5.9.6	
5.9.5	Updated to **7.4.28**
5.9.3/5.9.4	Updated to **7.4.19**
5.9.0	Updated to **7.4.6**
5.8.1	Updated to 5.6.35-pl1

- **NetClock 9300 and 9200 series:**
- **1232 VelaSyncs:**

CVE-2018-16451 (tcpdump -- security update)

- ➢ Refer to

Severity:

Products:

- ○ **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- ○ **Legacy VelaSync: ?**
- ○ **1200 SecureSync/9400s:** ?
- ○ **NetClock 9300 and 9200 series**: ?

CVE-2018-16230 (tcpdump -- security update)

- ➢ Refer to

Severity:

Products:

- ○ **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- ○ **Legacy VelaSync: ?**
- ○ **1200 SecureSync/9400s:** ?
- ○ **NetClock 9300 and 9200 series**: ?

CVE-2018-16229 (tcpdump -- security update)

- ➢ Refer to

Severity:

Products:

- ○ **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- ○ **Legacy VelaSync: ?**
- ○ **1200 SecureSync/9400s:** ?
- ○ **NetClock 9300 and 9200 series**: ?

CVE-2018-16228: tcpdump -- security update

- ➢ Refer to

Severity:

Products:

- ○ **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- ○ **Legacy VelaSync: ?**
- ○ **1200 SecureSync/9400s:** ?

- **NetClock 9300 and 9200 series**: ?

CVE-2018-16227 (tcpdump -- security update)

- Refer to

Severity:

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**

CVE-2018-15473 (OpenSSH vulnerability)

- **Refer to**:
- **Description**:

Severity:

Products:

- **VersaSyncs**
- **1232 VelaSyncs:**
- **1200 SecureSync/9400s:** OpenSSH was updated to 8.1p1 in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **NetClock 9300 and 9200 series**:

CVE-2018-14882: tcpdump -- security update

- Refer to

Severity:

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2018-14881: tcpdump -- security update

- Refer to

Severity:

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2018-14880: tcpdump -- security update

- Refer to

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2018-14879: tcpdump -- security update

- Refer to

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2018-14633 linux, linux-4.9 -- security update

- Refer to

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2018-14480 tcpdump -- security update

- Refer to

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2018-14469: tcpdump -- security update

- Refer to

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2018-14468: tcpdump -- security update

- Refer to

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2018-14467: tcpdump -- security update

- Refer to

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2018-14466: tcpdump -- security update

- Refer to

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2018-14465: tcpdump -- security update

- ➢ Refer to

Products:

- ○ **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- ○ **Legacy VelaSync: ?**
- ○ **1200 SecureSync/9400s:** ?
- ○ **NetClock 9300 and 9200 series**: ?

CVE-2018-14463: tcpdump -- security update

- ➢ Refer to

Products:

- ○ **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- ○ **Legacy VelaSync: ?**
- ○ **1200 SecureSync/9400s:** ?
- ○ **NetClock 9300 and 9200 series**: ?

CVE-2018-14462: tcpdump -- security update

- ➢ Refer to

Products:

- ○ **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- ○ **Legacy VelaSync: ?**
- ○ **1200 SecureSync/9400s:** ?
- ○ **NetClock 9300 and 9200 series**: ?

CVE-2018-10933 (libssh exploit)

- ➢ inquiry received 24 Oct 2018
- ➢ Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2018-10933 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10933

Description: A vulnerability was found in libssh's server-side state machine before versions 0.7.6 and 0.8.4. A malicious client could create channels without first performing authentication, resulting in unauthorized access.

Severity:

Products:

- **VersaSyncs**
  - ○ **N/A we do not use this affected package (per Ron Dries, 24 Oct 2018 "**I have asked engineering and they have confirmed that we use openssh and not libssh in SecureSync, VersaSync, and VelaSync")
- **2400 SecureSyncs**
  - ○ **N/A we do not use this affected package (per Ron Dries, 24 Oct 2018 "**I have asked engineering and they have confirmed that we use openssh and not libssh in SecureSync, VersaSync, and VelaSync")
- **1200 SecureSync/9400s:**
  - ○ **N/A we do not use this affected package (per Ron Dries, 24 Oct 2018 "**I have asked engineering and they have confirmed that we use openssh and not libssh in SecureSync, VersaSync, and VelaSync")
- **VelaSyncs**
  - ○ **N/A we do not use this affected package (per Ron Dries, 24 Oct 2018 "**I have asked engineering and they have confirmed that we use openssh and not libssh in SecureSync, VersaSync, and VelaSync")
- **NetClock 9300 and 9200 series:**
  - ○ **N**/A we do not use this affected package (per Ron Dries, 24 Oct 2018 "**I** have asked engineering and they have confirmed that we use openssh and not libssh in SecureSync, VersaSync, and VelaSync")

CVE-2018-14882 (Debian: CVE-2018-14882: tcpdump -- security update)

- ➢ Refer to

Products:

○ **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
○ **Legacy VelaSync: ?**
○ **1200 SecureSync/9400s:** ?
○ **NetClock 9300 and 9200 series**: ?

CVE-2018-14470 (: tcpdump -- security update)

- ➢ Refer to

Products:

○ **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
○ **Legacy VelaSync: ?**

- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2018-14464 (tcpdump -- security update)

- Refer to

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2018-14461 tcpdump -- security update)

- Refer to

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2018-14633 (Debian linux, linux-4.9 -- security update)

- Refer to

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2018-10933 (libssh exploit)

- inquiry received 24 Oct 2018
- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2018-10933 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10933

Description: A vulnerability was found in libssh's server-side state machine before versions 0.7.6 and 0.8.4. A malicious client could create channels without first performing authentication, resulting in unauthorized access.

Severity:

Products:

- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s: N/A we do not use this affected package (per Ron Dries, 24 Oct 2018 "**I have asked engineering and they have confirmed that we use openssh and not libssh in SecureSync, VersaSync, and VelaSync")
- **NetClock 9300 and 9200 series**: **N/A we do not use this affected package (per Ron Dries, 24 Oct 2018 "**I have asked engineering and they have confirmed that we use openssh and not libssh in SecureSync, VersaSync, and VelaSync")
- **VersaSyncs N/A we do not use this affected package (per Ron Dries, 24 Oct 2018 "**I have asked engineering and they have confirmed that we use openssh and not libssh in SecureSync, VersaSync, and VelaSync")
- **VelaSyncs N/A we do not use this affected package (per Ron Dries, 24 Oct 2018 "**I have asked engineering and they have confirmed that we use openssh and not libssh in SecureSync, VersaSync, and VelaSync")

CVE-2018-10549 / CVE-2018-10548 / CVE-2018-10546 / CVE-2018-10545 (PHP vulnerability)

- **Refer to**:

Description:

Severity:

Products:

- **2400 SecureSyncs/VersaSyncs**

2400 S/S Version	PHP version
1.4.3	Updated to 8.0.20
1.4.1	7.4.15
1.2.1 and 1.2.2	Updated to **7.4.4**
1.2.0	? 5.6.35-pl1 ?

- **1232 VelaSyncs:**
- **1200 SecureSync/9400s:** PHP was updated to 7.4.6 in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **NetClock 9300 and 9200 series**:

CVE-2018-10105: tcpdump -- security update

- ➢ Refer to

Products:

- ○ **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- ○ **Legacy VelaSync: ?**
- ○ **1200 SecureSync/9400s:** ?
- ○ **NetClock 9300 and 9200 series**: ?

CVE-2018-10103 (tcpdump -- security update)

- ➢ Refer to

Products:

- ○ **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- ○ **Legacy VelaSync: ?**
- ○ **1200 SecureSync/9400s:** ?
- ○ **NetClock 9300 and 9200 series**: ?

CVE-2018-5968 (Jackson DataBind - A deserialization of untrusted data vulnerability")

- ➢ Refer to: https://nvd.nist.gov/vuln/detail/CVE-2018-5968 https://security-tracker.debian.org/tracker/CVE-2018-5968 https://medium.com/@cowtowncoder/on-jackson-cves-dont-panic-here-is-what-you-need-to-know-54cd0d6e8062

Description: FasterXML jackson-databind through 2.8.11 and 2.9.x through 2.9.3 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 and CVE-2017-17485 deserialization flaws. This is exploitable via two different gadgets that bypass a blacklist.

Severity:

Products:

- **1200 SecureSync/9400s: N/A (per dave Sohn on 9 April 2018. we do not use this affected package)**
- **Legacy VelaSync: ?**
- **NetClock 9300 and 9200 series:**
  - N/A - we do not use this affected package

CVE-2018-5732 (DHCP)

- ➢ Refer to: https://nvd.nist.gov/vuln/detail/CVE-2018-5732

Severity:

Products:

- **2400 SecureSyncs**
- **1200 SecureSync/9400s:**

- versions 5.7.3 and below are affected. Fixed in v5.8.0
  (per the v5.8.0 Release Notes "DHCP was updated to 6.1 correcting the following:CVE-2018-5732")

- **Legacy VelaSync**: ?

- **NetClock 9300 and 9200 series:???**

CVE-2018-5407: (Port Smash / Hyper-Threading)

- Refer to SF case 179315
- Refer to: https://access.redhat.com/security/cve/cve-2018-5407 and https://nvd.nist.gov/vuln/detail/CVE-2018-5407

Description: A microprocessor side-channel vulnerability was found on SMT (e.g, Hyper-Threading) architectures. An attacker running a malicious process on the same core of the processor as the victim process can extract certain secret information

This is a timing side-channel flaw on processors which implement SMT/Hyper-Threading architectures. It can result in leakage of secret data in applications such as OpenSSL that has secret dependent control flow at any granularity level. In order to exploit this flaw, the attacker needs to run a malicious process on the same core of the processor as the victim process.

Mitigation (Excerpted from above sites, on 1 Jan 2019)

At this time Red Hat Engineering is working on patches to address this issue. Until fixes are available, users are advised to review the guidance supplied in the L1 Terminal Fault vulnerability article: https://access.redhat.com/security/vulnerabilities/L1TF and decide what their exposure across shared CPU threads are and act accordingly.

Severity:

Products: (Note: KW emailed apps team on 1 Jan, 2019 to see if our products are affected, based on the guidance referenced in the link above)

- **1200 SecureSync/9400s: ?**

  Email from Danny L to Roots: Keith had pointed out this is the relevant CVE for PORTSMASH. https://nvd.nist.gov/vuln/detail/CVE-2018-5407

  Our hardware, the ETX module (both old and new) does not feature clustered multi-thread (CMT) so is not affected by Port Smash.

  However, our software (Firmware V5.8.3 is using openSSL V1.0.2o so it is still venerable.

  We will most likely upgrade our openSSL > 1.0.2q to mitigate this venerability.

- **Prisma VelaSyncs: ?**
- **NetClock 9300 and 9200 series: ???**

CVE-2018-5381, CVE-2018-5380, CVE-2018-5379, CVE-2018-5378 (Quagga BGP for NTP over Anycast mode)

- ➢ Refer to links: CVE-2018-5378, CVE-2018-5379, CVE-2018-5380, CVE-2018-5381

  https://nvd.nist.gov/vuln/detail/CVE-2018-5379

Description: The Quagga BGP daemon (bgpd) prior to version 1.2.3 can double-free memory when processing certain forms of UPDATE message, containing cluster-list and/or unknown attributes. A successful attack could cause a denial of service or potentially allow an attacker to execute arbitrary code.

Severity:

Products:

- **1200 SecureSync/9400s: versions prior to v.8.0 are affected. Version 5.8.0 update fixes**
  - **Per the Version 5.,8.0 Release Notes: "Quagga** was **updated to 1.2.4** correcting the following:CVE-2018-5378, CVE-2018-5379, CVE-2018-5380, CVE-2018-5381"
- **Legacy VelaSync**: ?

- **NetClock 9300 and 9200 series:**
  - believe N/A, as they do not use BGP (used for NTP over anycast mode)

CVE-2018-4878 (Adobe Flash player)

- ➢ Refer to https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4878

Per Dave Sohn (7 Feb 18) "We don't have anything working with Adobe Flash"

Products:

- **1200 SecureSync/9400s:** N/A
- **Legacy VelaSync**: N/A
- **NetClock 9300 and 9200 series:** N/A

CVE-2018-3646/CVE-2018-3615/CVE-2018-3620 (similar to Spectre/Meltdown)

per Dave Sohn (7 Sept 2018) All three of these vulnerabilities appear to be specific to Intel processors, which are not in use within the SecureSync.

- Refer to:

3646: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3646
https://access.redhat.com/security/cve/cve-2018-3646

Modern operating systems implement virtualization of physical memory to efficiently use available system resources and provide inter-domain protection through access control and isolation. The L1TF issue was found in the way the x86 microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization) in combination with handling of page-faults caused by terminated virtual to physical address resolving process. As a result, an unprivileged attacker could use this flaw to read privileged memory of the kernel or other processes and/or cross guest/host boundaries to read host memory by conducting targeted cache side-channel attacks.

3620: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3620
https://access.redhat.com/security/cve/cve-2018-3620

Modern operating systems implement virtualization of physical memory to efficiently use available system resources and provide inter-domain protection through access control and isolation. The L1TF issue was found in the way the x86 microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization) in combination with handling of page-faults caused by terminated virtual to physical address resolving process. As a result, an unprivileged attacker could use this flaw to read privileged memory of the kernel or other processes and/or cross guest/host boundaries to read host memory by conducting targeted cache side-channel attacks.

3615: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3615
https://access.redhat.com/security/cve/cve-2018-3615

Systems with microprocessors utilizing speculative execution and Intel software guard extensions (Intel SGX) may allow unauthorized disclosure of information residing in the L1 data cache from an enclave to an attacker with local user access via a side-channel analysis.

Products:

per Dave Sohn (7 Sept 2018) All three of these vulnerabilities appear to be specific to Intel processors, which are not in use within the SecureSync.

- **Legacy VelaSync:** ?
- **1200 SecureSync/9400s**
- **NetClock 9300 and 9200 series: ?**

CVE-2018-0739 (Denial of Service attack)

- Refer to: https://nvd.nist.gov/vuln/detail/CVE-2018-0739

Description: Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).

Severity:

Products:

- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s** Fixed in **version 5.8.0** (per the v5.8.0 Release Notes **"**OpenSSL was updated to 1.0.2n correcting the following: CVE-2018-0739)
- **NetClock 9300 and 9200 series**: ?

CVE-2018-0732 (OpenSSL vulnerability)

- **Refer to**:
- **Description**:

Severity:

Products:

- **VersaSyncs**
- **1232 VelaSyncs:**
- **1200 SecureSync/9400s:** OpenSSL was updated to 1.0.2u in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.

CVE-2018-5407 (OpenSSL vulnerability)

- **Refer to**:
- **Description**:

Severity:

Products:

- **VersaSyncs**
- **1232 VelaSyncs:**

- **1200 SecureSync/9400s:** OpenSSL was updated to 1.0.2u in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.

CVE-2017-16939
The XFRM dump policy implementation in net/xfrm/xfrm_user.c in the Linux kernel before 4.13.11 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted SO_RCVBUF setsockopt system call in conjunction with XFRM_MSG_GETPOLICY Netlink messages.

- Refer to https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-CVE-2017-16939

Severity:

Products:

- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ??
- **NetClock 9300 and 9200 series**: I highly suspect all software versions 3.6.7 and below??

CVE-2017-16650 (Linux Kernel ‘drivers/net/usb/qmi_wwan.c’ Local Denial of service)

A Vulnerability in Linux Kernel allows local users to cause a denial of service (divide-by-zero error and system crash) or possibly have unspecified other impact via a crafted USB device.

- Refer to https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-16650

Severity:

Products:

- **Legacy VelaSync: ??**
- **1200 SecureSync/9400s:** ??
- **NetClock 9300 and 9200 series**: I highly suspect all software versions 3.6.7 and below??

CVE-2017-15299 (Linux Kernel “key create or update()” NULL Pointer Dereference Vulnerability)
- A Vulnerability in Linux Kernel exploited to trigger a NULL pointer dereference and cause kernel crash

Affected systems

- Linux kernel 3.16.x
- Linux kernel 3.2.x
- Linux kernel 4.1.x
- Linux kernel 4.13.x
- Linux kernel 4.4.x
- Linux kernel 4.9.x

http://seclists.org/oss-sec/2017/q4/82
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15299
https://cdn.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.16.50
https://cdn.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.2.95
https://cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.1.46
https://cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.4.95
https://cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.9.59

https://cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.13.10
https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable.git/commit/?id=4fbd8d194f06c8a3fd2af1ce560ddb31f7ec8323

Severity:

Products:

- **Legacy VelaSync: ??**
- **1200 SecureSync/9400s:** ??
- **NetClock 9300 and 9200 series**: I highly suspect all software versions 3.6.7 and below??

CVE-2017-15102 - A Vulnerability in Linux Kernel allows local users (who are physically proximate for inserting a crafted USB device) to gain privileges by leveraging a write-what-where condition that occurs after a race condition and a NULL pointer dereference.

More Information

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15102
https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.4.24
https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.7.7
https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.8.1
https://www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.16.40
https://www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.10.105
https://www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.2.85

Products:

- **Legacy VelaSync: ??**
- **1200 SecureSync/9400s:** ??
- **NetClock 9300 and 9200 series**: I highly suspect all software versions 3.6.7 and below??

CVE-2017-15671, CVE-2017-15804, CVE-2017-16997, CVE-2017-14062, CVE-2018-1000001, CVE-2018-6485, CVE-2018-6551

- Refer to

CVE-2017-14062, CVE-2017-15670, CVE-2017-15671, CVE-2017-15804, CVE-2017-16997, CVE-2018-1000001, CVE-2018-6485, CVE-2018-6551

Severity:

Products:

- **Legacy VelaSync: ??**
- **1200 SecureSync/9400s:** fixed in v5.8.0 (per the v5.8.0 release notes: "**glibc** was updated to **2.25-r12** correcting the following: CVE-2017-14062, CVE-2017-15671, CVE-2017-15804, CVE-2017-16997, CVE-2018-1000001, CVE-2018-6485, CVE-2018-6551")
- **NetClock 9300 and 9200 series**: I highly suspect all software versions 3.6.7 and below??

CVE-2017-10911 Update for linux kernel Xen Block interface information disclosure vulnerability

The make_response function in drivers/block/xen-blkback/blkback.c in the Linux kernel before 4.11.8 allows guest OS users to obtain sensitive information from host OS (or other guest OS) kernel memory by leveraging the copying of uninitialized padding fields in Xen block-interface response structures, aka XSA-216.

- Refer to https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10911

Severity:

Products:

- **Legacy VelaSync: Fixed in basepackage 1.9 (TK versions 7.2.9 and above)**
- **1200 SecureSync/9400s:** ??
- **NetClock 9300 and 9200 series**: I highly suspect all software versions 3.6.7 and below??

CVE-2017-1000364, CVE-2017-1000365, CVE-2017-1000370, CVE-2017-1000371 and CVE-2017-1000379 (Stack Clash)

- Refer to sites such as: https://www.qualys.com/2017/06/19/stack-clash/stack-clash.txt or https://www.qualys.com/2017/06/19/stack-clash/stack-clash.txt

Products:

- **Legacy VelaSync: Fixed in basepackage 1.9 (TK versions 7.2.9 and above)**
- **1200 SecureSync/9400s:** Fixed in update **version 5.7.3** (limited release. Not yet cut into production as of 6 Feb, 2018)

  From the v5.7.3 release notes: "Kernel was updated from 4.4.26 to 4.4.87"
- **NetClock 9300 and 9200 series**: I highly suspect all software versions 3.6.7 and below??

CVE-2017-12617 (tomcat: Remote Code Execution bypass for CVE-2017-12615)

- Refer to sites such as https://access.redhat.com/security/cve/cve-2017-12617

When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81 with HTTP PUTs enabled (e.g. via setting the readonly initialization parameter of the Default servlet to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.

Severity:

Products:

- **Legacy VelaSync: Fixed in basepackage 1.9 (TK versions 7.2.9 and above)**
- **1200 SecureSync/9400s:** ??
- **NetClock 9300 and 9200 series**: I highly suspect all software versions 3.6.7 and below??

CVE-2017-11108 CVE-2017- (11541-11544), CVE-2017-(12893-12902), CVE-2017-(12985-13055), CVE-2017- (13687-13690), CVE-2017-13725 (tcpdump?)

- Refer to sites such as:

Severity:

Description:

Products:

- **Legacy VelaSync:** ??
- **1200 SecureSync/9400s:** v5.7.2 and below are affected. Fixed in v5.7.3 update
  From the v5.7.3 release notes: "**tcpdump** was updated to 4.9.2 to resolve many vulnerabilities"

- **NetClock 9300 and 9200 series**: I highly suspect **NO version is** affected (really don't believe they have Apache Struts plugin installed)

CVE-2017-10684, CVE-2017-10685, CVE-2017-11112, CVE-2017-11113, CVE-2017-13728, CVE-2017-13729, CVE-2017-13730, CVE-2017-13731, CVE-2017-13732, CVE-2017-13733, CVE-2017-13734, CVE-2017-16879

- ➢ Refer to the following links:

- CVE-2017-10684, CVE-2017-10685, CVE-2017-11112, CVE-2017-11113, CVE-2017-13728, CVE-2017-13729, CVE-2017-13730, CVE-2017-13731, CVE-2017-13732, CVE-2017-13733, CVE-2017-13734, CVE-2017-16879

Severity:

Products:

- **1200 SecureSync/9400s** versions 5.7.3 and below are affected.   Fixed in version 5.8.0

  (per the V5.8.0 Release notes: "ncurses was updated to 6.1 correcting the following: CVE-2017-10684, CVE-2017-10685, CVE-2017-11112, CVE-2017-11113, CVE-2017-13728, CVE-2017-13729, CVE-2017-13730, CVE-2017-13731, CVE-2017-13732, CVE-2017-13733, CVE-2017-13734, CVE-2017-16879)

- **Legacy VelaSync:** ??

- **NetClock 9300 and 9200 series**: I highly suspect all software versions 3.6.7 and below??

CVE-2017-9805 (Apache Struts 2 REST plugin Remote Code Execution)

- ➢ Refer to sites such as: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9805
- ➢ Refer to Salesforce case
- ➢ New Vulnerability announced/Linux update patches started being made available ~

Description: "a new critical Apache Struts 2 vulnerability was announced which allows remote attackers to execute arbitrary commands on the server".

Severity:

Products:

- **Legacy VelaSync:** I highly suspect **NO version is** affected (really don't believe they have Apache Struts plugin installed)**1200 SecureSync/9400s:** at least v5.7.0 and below are **NOT** affected. Per Dave Sohn (7 Sept 17) "We do not use Apache struts plugin.

- **NetClock 9300 and 9200 series**: I highly suspect **NO version is** affected (really don't believe they have Apache Struts plugin installed)

CVE-2017-9798 (OptionsBleed)

- **Refer to sites such as**: https://nvd.nist.gov/vuln/detail/CVE-2017-9798
- Refer to Salesforce case: 173604

Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. **This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27.** The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

Vulnerable: Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27.

Severity:

Products:

- **Prisma VelaSync: at least versions 1.0.0 and 1.1.0 use Apache 2.4.25 (they are affected)**
  Status update email from Sadie to customer (after input from Dave S) (9 Jan 2019) "The VelaSync 1232 does not have the directives set (within Apache) to be vulnerable to this issue and users do not have access to change this variable- **so the VelaSync 1232 is unaffected by CVE-2017-9798.** To ensure this issue does not affect any future development on this platform, Orolia will be patching Apache in a future firmware release, roughly targeting mid-year."

  1200 SecureSync/9400s: at least 5.8.3 (and below) have ***Apache version 2.2.34*** and therefore appear to be affected, until a post 5.8.3 release updates Apache (per Ryan on 8 Jan 2019. prior to v5.8.3 release, "5.8.3 still contains Apache 2.2.34"). Ryan said he will create a JIRA case for post 5.8.3 to update Apache.
  See above status update email from Sadie about Prisma VelaSyncs

- NetClock 9300 and 9200 series**: I highly suspect all software versions ???**
- **Legacy VelaSync:** ???

CVE-2017-9445 (associated with systemd)

- Refer to sites such as: https://www.mail-archive.com/gentoo-commits@lists.gentoo.org/msg278345.html
- Refer to Salesforce case 25842
- New Vulnerability announced/Linux update patches started being made available ~1 July 2017

Description: In **systemd** through 233, certain sizes passed to dns_packet_new in systemd-resolved can cause it to allocate a buffer that's too small. A malicious DNS server can exploit this via a response with a specially crafted TCP payload to trick systemd-resolved into allocating a buffer that's too small, and subsequently write arbitrary data beyond the end of it.

Severity:

Products:

- **Legacy VelaSync: At least 7.2.7 and below (7.2.7 was released 23 Jun, 17)?**
- **1200 SecureSync/9400s:** at least v5.7.0 and below are **NOT** affected. Per Dave Sohn (5 July 17) "We do not currently use systemd on SecureSync".

  Response back to this customer- Regarding case number 25842, our SecureSync Product Manager has just notified me that the SecureSync does not use "systemd", which this particular potential vulnerability is directly associated with. So, this CVE is not applicable to the Spectracom SecureSyncs ☺!
- **NetClock 9300 and 9200 series**: I highly suspect all software versions 3.6.7 and below??

CVE-2017-7679, CVE-2017-7668, CVE-2017-3169, CVE-2017-3167 (mod_mime)

Refer to:

CVE-2017-7679: https://nvd.nist.gov/vuln/detail/CVE-2017-7679
In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

CVE-2017-7668: https://nvd.nist.gov/vuln/detail/CVE-2017-7668

The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.

CVE-2017-3169 https://nvd.nist.gov/vuln/detail/CVE-2017-3169

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.

CVE-2017-3167: https://nvd.nist.gov/vuln/detail/CVE-2017-3167

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

.

Susceptible: NTP versions prior to v4.2.8.p11

Severity:

Products:

- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** fixed in version 5.8.0 (May 2018).
- **Per the 5.8.0 Release Notes "***Apache was updated to 2.2.34 correcting the following*: CVE-2017-7679, CVE-2017-7668, CVE-2017-3169, CVE-2017-3167"
- **NetClock 9300 and 9200 series**: all versions 3.6.7 and below

----

CVE-2017-7494 Samba: loading shared modules from any path in the system leading to RCD

Description A remote code execution flaw was found in Samba. A malicious authenticated samba client, having write access to the samba share, could use this flaw to execute arbitrary code as root.

Samba: "Samba is an Open Source/Free Software suite that provides seamless file and print services to SMB/CIFS clients." Samba is freely available, unlike other SMB/CIFS implementations, and allows for interoperability between Linux/Unix servers and Windows-based clients.

Refer to: https://access.redhat.com/security/cve/CVE-2017-7494

Susceptible: Red Hat (samba)" variants, such as:

- "Red Hat Enterprise (samba)"
- "Red Hat Enterprise (samba)"
- "Red Hat Gluster (samba)"

Email from Paul M (5/30/17) regarding SecureSyncs.9400s (as of at least v5.7.0) and 9300s. No the shipping product does NOT use samba. We can use it for development on the VMs, but shipping SecureSync's do NOT use this.

Severity:

Products:

- **Legacy VelaSync: Not applicable???**
- **1200 SecureSync/9400s:** Not applicable?
- **NetClock 9300 and 9200 series**: Not applicable?

Meltdown and Spectre vulnerabilities

A) Meltdown vulnerability

CVE-2017-5754

- Refer to sites such as: https://nvd.nist.gov/vuln/detail/CVE-2017-5754

Severity:

Products:

- **Legacy VelaSync: ??**
- **1200 SecureSync/9400s:** N/A. Per the v5.8.0 Release Notes: "System is not vulnerable to Meltdown CVE-2017-5754)

  Salesforce chatter:
  https://orolia.my.salesforce.com/_ui/core/userprofile/UserProfilePage?u=005C0000004CriB&tab=sfdc.ProfilePlatformFeed&fId=0D50h00004nmTNO&s1oid=00D80000000aMdF&s1nid=000000000000000&emkind=chatterGroupDigest&s1uid=00580000001p7IW&emtm=1515216072646&fromEmail=1&s1ext=0
- **NetClock 9300 and 9200 series**: ?

B) "Spectre vulnerabilities"

CVE-2017-5753 and CVE-2017-5715 (Spectre vulnerabilities)

- Refer to sites such as:

- https://meltdownattack.com/
- https://nvd.nist.gov/vuln/detail/CVE-2017-5715

Description: Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

Severity:

Products:

- **Legacy VelaSync:**
  Email from Cort (4 Jan 18 to a mutual customer) We don't know for certain yet but given that these flaws impact every Intel processor made in the last 10 years it's very likely. We're monitoring this of course and the fix will likely be an updated basepackage which updates the kernel.

- **1200 SecureSync/9400s: Mitigated starting in version 5.8.0 (from the v5.8.0 Release Notes"**
  Kernel was updated to 4.14.34 resolving Spectre vulnerabilities)
  Note: the fixes applied in versions 5.8.0 to address Spectre inherently increase the CPU usage. Refer to the CPU usage section of the SecureSync tech note for more details:

announcement on our website: https://support.spectracom.com/bulletins/spectre-and-meltdown-vulnerabilities-cve-2016-5715-cve-2017-5753-cve-2017-5754

Salesforce chatter:
https://orolia.my.salesforce.com/_ui/core/userprofile/UserProfilePage?u=005C0000004CriB&tab=sfdc.ProfilePlatformFeed&fId=0D50h00004nmTNO&s1oid=00D80000000aMdF&s1nid=000000000000000&emkind=chatterGroupDigest&s1uid=00580000001p7IW&emtm=1515216072646&fromEmail=1&s1ext=0

- **NetClock 9300 and 9200 series: ?**

CVE-2017-5689 (AMT and ME architecture for management in Intel processors.

Severity:

Products:

- **Legacy VelaSync: See email above from Cort below**
  Email from Cort (8 May 17) Vulnerability CVE-2017-5689 was recently announced. It is related to the AMT and ME architecture for management in Intel processors.
  TimeKeeper Enterprise Grandmaster systems and TimeKeeper Pocket Grandmaster systems are not susceptible to this vulnerability but we will continue to monitor the issue as more information becomes available. We will also continue to update you about any impact on TimeKeeper and FSMLabs.

  If you have any questions or concerns please feel free to contact support@fsmlabs.com

- **1200 SecureSync/9400s:**?
- **NetClock 9300 and 9200 series**:?

CVE-2017-3735, CVE-2017-3736, CVE-2017-3737 and CVE-2017-3738

- Refer to:

Severity:

Products:

- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** versions 5.7.2 and below are affected (fixed in v5.7.3 update, which updated OpenSSL to **version 1.0.2n)**

  From the v5.7.3 release notes: **OpenSSL** was updated to 1.0.2n correcting the following:

  - CVE-2017-3735, CVE-2017-3736, CVE-2017-3737, CVE-2017-3738

- **NetClock 9300 and 9200 series**: ?

CVE-2017-3732 (OpenSSL vulnerability)

- Refer to https://www.openssl.org/news/secadv/20170126.txt
- "OpenSSL 1.1.0 users should upgrade to 1.1.0d.   OpenSSL 1.0.2 users should upgrade to 1.0.2k.

Products:

- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** versions 5.6.0 and below are affected (fixed in v5.7.0 update which updated OpenSSL to **v1.0.2k**, per JIRA ticket SSS-218)
- **NetClock 9300 and 9200 series**: ?

CVE-2017-3731 (OpenSSL vulnerability)

- Refer to https://www.openssl.org/news/secadv/20170126.txt
- "Users who have not disabled that algorithm should update to 1.0.2k"

Severity:

Products:

- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** versions 5.6.0 and below are affected (fixed in v5.7.0 update which updated OpenSSL to **version 1.0.2k**, per JIRA ticket SSS-218)
- **NetClock 9300 and 9200 series**: ?

CVE-2017-3730 (OpenSSL vulnerability)

- Refer to https://www.openssl.org/news/secadv/20170126.txt
- "OpenSSL 1.1.0 users should upgrade to 1.1.0d"

Severity:

Products:

- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** versions 5.6.0 and below are affected (fixed in v5.7.0 update which updated OpenSSL to **version 1.0.2k**, per JIRA ticket SSS-218)
- **NetClock 9300 and 9200 series**: ?

CVE-2016-10150 (Debian linux -- security update)

- Refer to

Severity:

Products:

- **1232 Velasyncs (refer to Salesforce Case 219165, reported in v1.2.0)**
- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** ?
- **NetClock 9300 and 9200 series**: ?

CVE-2016-8743 / CVE-2016-8740

- **Refer to**:
- **Description**:

Severity:

Products:

- **VersaSyncs**
- **1232 VelaSyncs:**
- **1200 SecureSync/9400s:** Apache was updated to 2.4.41 in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.

CVE-2016-7055 (OpenSSL vulnerability)

- Refer to https://www.openssl.org/news/secadv/20170126.txt
- OpenSSL 1.0.2 users should upgrade to **1.0.2k**

Severity:

Products:

- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** versions 5.6.0 and below are affected (fixed in v5.7.0 update which updated OpenSSL to **version 1.0.2k**, per JIRA ticket SSS-218)
- **NetClock 9300 and 9200 series**: ?

CVE-2017-5638 "Apache Struts2 Content-Type Input Validation Code Execution Vulnerability."

- **Refer to:** https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638

Description: The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 mishandles file upload, which allows remote attackers to execute arbitrary commands via a #cmd= string in a crafted Content-Type HTTP header, as exploited in the wild in March 2017.

Severity:

Susceptible:

Products:

- **Legacy VelaSync: ???**
- **1200 SecureSync/9400s:** Not applicable
- **NetClock 9300 and 9200 series**: Not applicable

Email from Paul Myers (16 Mar 17)

https://struts.apache.org/
We don't include apache struts.
I don't see apache struts as part of Gentoo anyway.
We use apache web server.

CVE-2016-5387

- **Refer to**:

Description:

Severity:

Products:

- **VersaSyncs**
- **1232 VelaSyncs:**
- **1200 SecureSync/9400s:** Apache was updated to 2.4.41 in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.

CVE-2016-5195 “Kernel Local Privilege Escalation” (AKA “Dirty COW”)

Refer to: https://bugs.gentoo.org/show_bug.cgi?id=597624 and
https://access.redhat.com/security/vulnerabilities/2706661

Red Hat Product Security has been made aware of vulnerability in the Linux kernel that has been assigned CVE-2016-5195. This issue was publicly disclosed on **October 19, 2016** and has been rated as Important.

Background Information

A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.

This could be abused by an attacker to modify existing setuid files with instructions to elevate privileges. An exploit using this technique has been found in the wild.

Email from Paul Myers (21 Oct 16) Keith, This is the impact is as below. The user has to be a local user on the box. SO only customers, Spectracom staff can exploit this with accounts ON the SecureSync. We are vulnerable INSIDER attacks.
We are vulnerable already to anyone with physical access to the SecureSync anyway for insider attacks. This allows ‘remote’ network authorized users to attack on the network. Attackers with NO login access have no advantage using this that I can see unless they can run code without logging in that they inject.

Paul
An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.
This flaw allows an attacker with a local system account to modify on-disk binaries, bypassing the standard permission mechanisms that would prevent modification without an appropriate permission set.

http://dirtycow.ninja/

What is the CVE-2016-5195?

CVE-2016-5195 is the official reference to this bug. CVE (Common Vulnerabilities and Exposures) is the Standard for Information Security Vulnerability Names maintained by MITRE.

Why is it called the Dirty COW bug?

"A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system."
(RH https://bugzilla.redhat.com/show_bug.cgi?id=1384344#)

https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
https://github.com/dirtycow/dirtycow.github.io/wiki/PoCs

Email from Paul M (21 Oct 16) Thanks for looking… I was looking into this, but I don’t think this can be turned around quickly and am not committing to it for this 5.5.0 release at this time.

Linus Torvalds, the creator of linux and primary kernel maintainer was involved in its creation and it has been around 9 years. I would be surprised if we are not affected.

https://lkml.org/lkml/2016/10/19/860

However, keep in mind we have not tried to recreate it and our other measures may provide enough protection to minimize the exploitation, such as I ‘think’ a user has to be logged in or have access to raise their priority to root.

Please add what you found to your SAP ticket.

The key question is if the user is prevented from logging in to the webpage or command line can we NOT be susceptible. If the user must be logged in then we are only at risk to an insider attack.

This link shows how to detect it on RedHat.

https://bugzilla.redhat.com/show_bug.cgi?id=1384344

Knowledge base article on our website for this potential vulnerability

http://support.spectracom.com/articles/FAQ/Dirty-COW-Vulnerability?&category=NetClock_Model_9400_Series&

Email Keith sent (7 Nov 16): You had inquired about the recent report of the "dirty COW" potential vulnerability (CVE-2016-5195) and how it may relate to Spectracom time servers.

I wanted to let you know that our software engineers have since published a knowledge base article on our website, providing information on this potential vulnerability. To review this article, please visit us at: http://support.spectracom.com/articles/FAQ/Dirty-COW-Vulnerability?&category=NetClock_Model_9400_Series&

Severity:

Products:

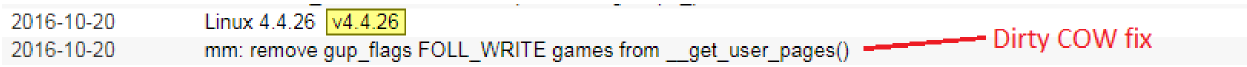
- **Legacy VelaSync: Fixed in basepackage version 1.8 (starting with TK version 7.2.3) Basepackage versions prior to v1.8 are susceptible.**

1200 SecureSync/9400s: Fixed in v5.7.0 (versions 5.6.0 and below are susceptible)

From the kbb on our website (link further above): "A fix for this vulnerability was implemented in June 2017, with the 5.7.0 SW release as part of a Linux Kernel update."

Status update, per Ryan Johnson (6 July 17) for SF case 25893

"Dirty COW" is resolved in 5.7.0. 5.7.0 runs Linux kernel version 4.4.26 which I verified contains the "Dirty COW" fix in the Gentoo release: https://gitweb.gentoo.org/proj/linux-patches.git/commit/?h=4.4&id=b34b17f4fe52530b679cbb066e4dbff4a9dd160d



```
2016-10-20          Linux 4.4.26 v4.4.26
2016-10-20          mm: remove gup_flags FOLL_WRITE games from __get_user_pages()
```

Dirty COW fix

https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable.git/log/?h=linux-4.4.y&ofs=2100

Why do they believe it's still present?

BTW, the full version info for 4.4.26 is as follows:

VERSION = 4
PATCHLEVEL = 4
SUBLEVEL = 26
EXTRAVERSION =
NAME = Blurry Fish Butt

- **NetClock 9300 and 9200 series**:
  - No software updates are required (or expected) for these products. Refer to the link above to the associated knowledge base article (discusses the need to maintain 'security' of account login passwords).

FAQs about Dirty COW (Replies in red from Dave Lorah, 8 Nov 16)

- When is a software version that fixes this issue planned. A firmware update is not required to mitigate the risk from this vulnerability. As long as the access to the equipment is password protected an attacker cannot login to exploit the vulnerability.

Status update (17 Mar 17) update version 5.7.0 (expected ~Apr 2017) for SecureSyncs/9400s is expected to fully eliminate this CVE.

- Will NetClock 9300/9200 get such a new software version as well? No new firmware updates are planned for the 9200/9300 series NetClocks. These devices are password-protected, so the vulnerability is not applicable.
- How can password rules/aging be configured on the devices. Changing the passwords from defaults to ones of your own making will mitigate the vulnerability. Password management is done in the SecureSync from the Management-> Authentication – > **Security Policy** page of the web UI.

CVE-2016-4979

- **Refer to**:
- **Description**:

Products:

- **VersaSyncs**
- **1232 VelaSyncs:**
- **1200 SecureSync/9400s:** Apache was updated to 2.4.41 in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.

CVE-2016-4049 “buffer overflow in bgpd” (related to Quagga)

Products:

- **Legacy VelaSync: ???**
- **1200 SecureSync/9400s:** Software versions 5.4.1 and below may potentially be affected. **Version 5.4.5** updated Quagga to newer version to address this CVE.
- **NetClock 9300 and 9200 series**: Software versions 3.6.7 and below???

CVE-2016-3115

It was discovered that the OpenSSH server did not sanitize data received in requests to enable X11 forwarding. An authenticated client with restricted SSH access could possibly use this flaw to bypass intended restrictions.

Susceptible: OpenSSH versions prior to v 7.2p1.

Products:

- **Legacy VelaSync: ???**
- **1200 SecureSync/9400s:** Software versions 5.4.1 and below may potentially be affected. **Version 5.4.5** updated OpenSSH to version 7.2p2 which addresses this CVE.
- **NetClock 9300 and 9200 series**: Software versions 3.6.7 and below???

CVE-2016-2342 “buffer overflow in bgpd” (related to Quagga)

Products:

1200 SecureSync/9400s: Software versions 5.4.1 and below may potentially be affected. **Version 5.4.5** updated Quagga to newer version to address this and other CVEs

- **Legacy VelaSync: ???**
- **NetClock 9300 and 9200 series**: Software versions 3.6.7 and below???

CVE-2016-2183/CVE-2016-6329 (DES and Triple DES ciphers, Birthday attack, Sweet 32/Sweet32 attack)

- Refer to:

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2183
https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info/

Description: The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain clear text data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.

Severity:

Products:

- **1232 VelaSyncs:**
  - Refer to Salesforce Case 183189 (Jan 2019)
  - Even though (as of at least v1.1.0) Prisma VelaSyncs do not have the ability to select between high level and medium level ciphers (like SecureSyncs have), this CVE does not apply to Velasyncs- **DES and TROPLE DES are not in the VelaSync's single cipher list**

Email from Dave Sohn (16 Jan 2019) I checked a 1.1.0 unit, and it also does not have the problem ciphers enabled, so no vulnerability.

(Keiths' reply, for software version 1.1.0, 16 Jan 2018) This CVE (**CVE-2016-2183/CVE-2016-6329)** pertaining only to the two specific SSL ciphers of **DES** and **TRIPLE DES,** does not apply to the VelaSyncs

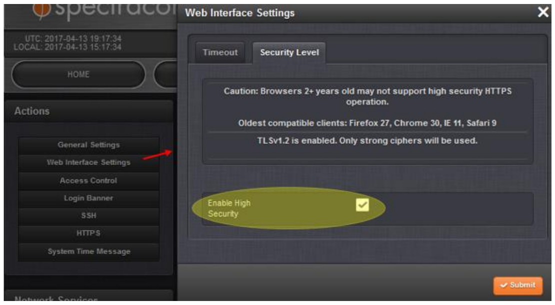
Our Engineers have now confirmed that neither of these two ciphers are in the VelaSync's list of available/usable ciphers. In order for this potential vulnerability to be present, these ciphers need to be listed in the unit's cipher list for potential selection. As they are not listed in the VelaSyncs cipher list, neither of these ciphers can be selected for use.

As neither of these DES ciphers exist in the VelaSync, your scanner tool appears to only be looking at a software package version to see if these two ciphers **MAY** be available in the ciphers list, instead of looking at the actual list of installed ciphers, causing the tool to alert to this vulnerability potentially being present (even though it's not)!

We expect to release a future software update for VelaSyncs, which will update package versions, alleviating this false detection alert.

- **1200 SecureSyncs and 9400s**: Update to **version 5.4.5 (or higher**) and configure SecureSync for High security ciphers only:
  - Enable High Security (Hi-Sec) to disable earlier versions of TLS. Refer to "**Disabling TLS**" in online SecureSync user guide at: http://manuals.spectracom.com/SS/Content/KB/TLSdisable.htm

Click “**Web interface Settings**” on the left side of the **Management** -> **Network Setup** page of the browser, and select the **Security Level** tab. Then select the “**Enable High Security”** checkbox to disable the referenced ciphers and press Submit.



Caution: Browsers 2+ years old may not support high security HTTPS operation.

Oldest compatible clients: Firefox 27, Chrome 30, IE 11, Safari 9

TLSv1.2 is enabled. Only strong ciphers will be used.

Email from Paul Myers (8 Sept 16) I think we are disabling these. OpenSSL 1.1.0 is not yet available to Gentoo. **https://packages.gentoo.org/packages/dev-libs/openssl**

-
- **Recommendation:**
- There is no good way to fix such design flaw. Users should config their TLS/SSL implementation to disable 3DES cipher suites.
- For compatible consideration, OpenSSL move 3DES cipher suites from HIGH to MEDIUM. But this still leave a door to exploit the vulnerability. So it recommended user to update to 1.1.0 or later in order to completely disable 3DES cipher suites. More information can be found at:
- https://sweet32.info/
- https://www.openssl.org/blog/blog/2016/08/24/sweet32/

- **NetClocks (9300 and 9200 series): ??**
- **Legacy VelaSync: ??**

CVE-2016-2161/CVE-1546

- **Refer to**:
- **Description**:

Products:

- **VersaSyncs**
- **1232 VelaSyncs:**
- **1200 SecureSync/9400s:** Apache was updated to 2.4.41 in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.

CVE-2016-0736

- **Refer to**:
- **Description**:

Products:

- **VersaSyncs**
- **1232 VelaSyncs:**
- **1200 SecureSync/9400s:** Apache was updated to 2.4.41 in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.

CVE-2015-2808: “ssl rc4 cipher suites supported vulnerability”

- General recommendation is to disable the RC4 (ARC4) cipher.
- Software update version 5.2.1 removed the RC4 cipher from the newer black/charcoal browser. But it’s still enabled in the classic interface browser in at least version 5.2.1.
- More on RC4 further below (including on how to mitigate this):

**RC4 (also known as ARC4 or ARCFour)

- **Refer to**: http://en.wikipedia.org/wiki/RC4
- **Refer to Mantis case 2293 (**http://cvsmantis.int.orolia.com/mantis/view_all_bug_page.php)
- ARCFour consists of ARCFour, ARCFour 128 and ARCFour 256
- ARCFour is known to be weak. ARCFour 128 and ARCFour 256 improve these ciphers by removing the less secure portion of the cipher.
- ARCFour was removed in the newer browser in version 5.2.1. but it's still enabled in the classic browser.
- ARCFour is enabled, but at the bottom of the cipher selection list, in at least version 5.0.0 and below
- ARCFour has been deleted (this will be incorporated in the release after version 5.0.0 (~Sept 2013).

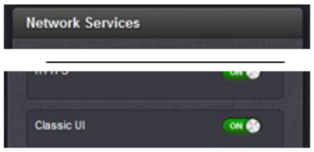
1200 SecureSync/9400 series status update for questions below:

- RC4 was initially removed in update version **5.0.1** (Refer to Mantis case 2293)
- RC4 was then inadvertently brought back into the software with version **5.1.5** (Refer to Mantis case 2918)
- RC4 was removed from the new browser in 5.2.1. But since it's still in the classic interface, the classic interface should be disabled, until the classic is removed via a future software update.

To mitigate potential vulnerabilities associated with RC4

- Update the software to at least version 5.2.1 to remove RC4 from the newer black browser.
- Until the classic interface has been removed from the software, disable the classic interface via the newer browser.

The classic interface web browser on port 8080 can be disabled in the bottom-left corner of the **Management** -> **Network** page of the newer black browser. It's the last slide switch in the "**Network Services**" list, labeled as "**Classic UI**" (as shown below). Note there is no need to reboot the SecureSync after sliding this switch to the OFF position.



Q. We need to disable RC4 for SSH (in SecureSync). Can you folks tell me how that can be done?

A. Reply from Paul Myers to Wade Sober (8 July 2013) If SSH users do NOT want RC4, please have Keith collect the customer requirements and enter a Mantis case.

Does the customer have a security reason why RC4 should be removed?
If it is generally applicable, we can consider removing it for all customers in a subsequent release.
I think this would require rebuilding of OpenSSL or less likely OpenSSH.
I don't recall an OpenSSH configuration operation to disable RC4.

For HTTP there might be such an option but they are referring to SSH correct?

A Another email from Paul Myers It seems like SSH2 is GOOD with ARCFOUR
http://www.openssh.org/security.html

OpenSSH was not vulnerable to the RC4 cipher password cracking, replay, or modification attacks. At the time that OpenSSH was started, it was already known that SSH 1 used the RC4 stream cipher completely incorrectly, and thus RC4 support was removed.

http://linux.die.net/man/5/sshd_config
ciphers described here

http://csce.uark.edu/~kal/info/private/ssh/ch03_09.htm
Restates RC4 is not useable with SSH1

CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2109, CVE-2016-2176, CVE-2016-0702, CVE-2016-0705, CVE-2016-0797, CVE-2016-0798, CVE-2016-0799, CVE-2016-0800 (all associated with OpenSSL version)

Products:

- **Legacy VelaSync: ???**
- **1200 SecureSync/9400s:** All of the above CVE's (associated with OpenSSL version) were fixed with the OpenSSL update to version 1.0.2h in the **version 5.4.5** update. Update the software to at least version 5.4.5 to fix.
- **NetClock 9300 and 9200 series**: Software versions 3.6.7 and below???

CVE-2015-7547 (glibc security and two bug fix update)

- Refer to Mantis case 3227
- Refer to: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7547 and https://rhn.redhat.com/errata/RHSA-2016-0175.html

Description:

A) Potential Security Vulnerability

- This issue was discovered by the Google Security Team and Red Hat

The glibc packages provide the standard C libraries (libc), POSIX thread libraries (libpthread), standard math libraries (libm), and the Name Server Caching Daemon (nscd) used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly.

A stack-based buffer overflow was found in the way the libresolv library performed dual A/AAAA DNS queries. A remote attacker could create a specially crafted DNS response which could cause libresolv to crash or, potentially, execute code with the permissions of the user running the library. Note: this issue is only exposed when libresolv is called from the nss_dns NSS service module.

B) This update also fixes the following two bugs:

1) The dynamic loader has been enhanced to allow the loading of more shared libraries that make use of static thread local storage. While static thread local storage is the fastest access mechanism it may also prevent the shared library from being loaded at all since the static storage space is a limited and shared process-global resource. Applications which would previously fail with "dlopen: cannot load any more object with static TLS" should now start up correctly. (BZ#1291270)
2) A bug in the POSIX realtime support would cause asynchronous I/O or certain timer API calls to fail and return errors in the presence of large thread-local storage data that exceeded PTHREAD_STACK_MIN in size (generally 16 KiB). The bug in librt has been corrected and the impacted APIs no longer return errors when large thread-local storage data is present in the application. (BZ#1301625)

Affected versions of glibc: ??

Products:

○ **Legacy VelaSync: ???**
More recent status update email from Cort (13 Apr 2016): The lastest copy of our software is 7.1.5 but 7.1.6 and basepackage 1.7 will include that fix the glibc vulnerability they're referring to. We expect that release soon.

Email from Cort (18 Feb 2016): “It is susceptible and we do plan to patch it. Hopefully in the next couple weeks after we've been able to test the change.”

○ **1200 SecureSync/9400s:** Software versions 5.3.1 and below may potentially be affected. Update version 5.4.0 prevents it from being potentially affected.
Email from Dave Sohn (17 Feb 2016): “SecureSync version 5.3.1 uses glibc 2.20. As it is difficult to say whether any of our packages might use the call, create the Mantis case. However, this will be fixed in 5.4.0 with the updated glibc with patches that we will be using.”

○ **NetClock 9300 and 9200 series**: Software versions 3.6.7 and below ???

CVE-2015-5621 (net-snmpd)

- Refer to Mantis case
- Refer to: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-5621 and https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5621
- **Description**: The snmp_pdu_parse function in snmp_api.c in net-snmp 5.7.2 and earlier does not remove the varBind variable in a netsnmp_variable_list item when parsing of the SNMP PDU fails, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted packet.

- **Affected software**: net-snmp versions 5.7.2 and below

Products:

- **1200 SecureSync/9400s:** Software versions 5.2.1 and below ???
- **NetClock 9300 and 9200 series**: Software versions 3.6.7 and below ???

CVE-2015-5600 (openssh – “MaxAuthTries bypass”)

- Refer to Mantis case 3106
- Refer to: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-5600 and http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5600
- **Description:** The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption)
- **Affected versions**: OpenSSH versions 6.9 and below (fixed in version 6.9p1)

Products:

- **1200 SecureSync/9400s:** software versions 5.2.1 and below (note version 5.3.0 updated OpenSSH to version 6.9p1)
- **NetClock 9300 and 9200 series:** at least software versions 3.6.7 and below

----

CVE-2015-5352 (OpenSSH Client Rejected `HostCertificate` Handling Vulnerability)

Refer to Mantis case 3106

Refer to: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-5352 and http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5352 and https://access.redhat.com/security/cve/CVE-2015-5352

Description: The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time windo

Affected versions: OpenSSH versions before 6.9 a (includes version 6.9p1 applied in software update version 5.3.0, Sept 2015)

Products:

- **Legacy VelaSync**
- **1200 SecureSync/9400s:** at least software versions 5.3.0 and below
- **NetClock 9300 and 9200 series:** at least software versions 3.6.7 and below

----

CVE-NONE-0791 (OpenSSH `PermitRootLogin` Security Bypass Vulnerability)

- Refer to Mantis case
- Refer to: http://www.saintcorporation.com/cgi-bin/demo_tut.pl?tutorial_name=OpenSSH_vulnerabilities.html and http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-NONE-0791
- **Description:** OpenSSH before 7.1 is prone to a vulnerability, which can be exploited by malicious, remote authenticated root user to bypass certain security restrictions. The vulnerability exists due to a logic error in "PermitRootLogin=prohibit-password" or "PermitRootLogin=without-password", depending on compile-time configuration. The vulnerability could allow password authentication to root and login to the target system.
- **Affected versions**: OpenSSH versions 7.0 and below (includes version 6.9p1 applied in software update version 5.3.0, Sept 2015)

Products:

- **1200 SecureSync/9400s:** at least software versions 5.3.0 and below
- **NetClock 9300 and 9200 series:** at least software versions 3.6.7 and below

----

CVE-2015-4000 ("TLS Diffie-Hellman Key Exchange Logjam vulnerability" for SSL/TLS)

- **Refer to**: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4000
- Refer to Mantis case 3059 for SecureSyncs and NetClock 9400s.
- **Description:** The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plain text or potentially violate the integrity of connections.

Solution: Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.
See Also http://weakdh.org/
Risk Factor: Medium
ulnerability Publication Date: May 20, 2015

Email from Keith (1 Jul 15) As this CVE is only associated with a man-in-the-middle (MITM) attack, do you or your customers normally access the time server via SSH or HTTPS from outside of the network it's on? Since the time server is only vulnerable to attack with an open connection to the network, our recommendation is to temporarily limit connections to the time server from external to the network it's connected with.

Products:

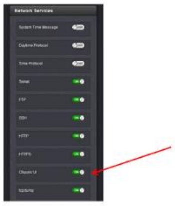
- **1200 SecureSync/9400s**: Software versions 5.2.1 and below, with an open SSH/HTTPS connection (susceptible to a Man-in-the-Middle (MITM) attack. Recommendation is to temporarily limit secure connections to the time server from external connections (such as from someone's home for example) where an attack in the middle is more likely.

  Version 5.3.0 is expected to remove the weak cipher associated with this CVE.

  Disable classic interface browser:

  Email from Keith to a customer (10 Mar 16) CVE-2015-2808 was addressed in the version 5.2.1 software update, when the classic interface browser has been disabled (this version of software added the ability to disable the classic interface browser access via a button in the newer black background web browser).

  With software version 5.2.1 or above installed, to disable access to the classic interface browser, in the newer browser navigate to the **Management** -> **Network** page. In the bottom-left corner, change the slider switch for "**Classic UI**" to the OFF position. Port "8080" is now closed, so the classic interface browser is no longer accessible.



Network Services

System Time Message OFF
Daytime Protocol OFF
Time Protocol OFF
Telnet ON
FTP ON
SSH ON
HTTP ON
HTTPS ON
Classic UI ON
tcpdump ON

  With the classic interface browser now disabled, all browser access will be via the newer black background web browser. Rescan and you should see this potential vulnerability is no longer present.

  Note that in order to use the newer web browser with Internet Explorer, IE may need to be updated to a much more recent version (we recommend IE 10 or higher) to be fully compatible with the newer browser.

- **NetClock 9300 and 9200 series**: Software versions 3.6.7 and below, with an open SSH/HTTPS connection (susceptible to a Man-in-the-Middle (MITM) attack. Recommendation is to limit secure connections to the NetClock from external connections (such as from someone's home for example) where an attack in the middle is more likely.

CVE-2015-3183

- **Refer to**:
- **Description**:

Products:

- **VersaSyncs**
- **1232 VelaSyncs:**
- **1200 SecureSync/9400s:** Apache was updated to 2.4.41 in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.

CVE-2015-1793

- Refer to https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1793 and https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1793
- **Applies only to**: OpenSSL 1.0.1n, 1.0.1o, 1.0.2b, and 1.0.2c

Summary: The X509_verify_cert function in crypto/x509/x509_vfy.c in **OpenSSL 1.0.1n, 1.0.1o, 1.0.2b, and 1.0.2c** does not properly process X.509 Basic Constraints cA values during identification of alternative certificate chains, which allows remote attackers to spoof a Certification Authority role and trigger unintended certificate verifications via a valid leaf certificate.

Products:

- **Legacy VelaSync ?**
- **1200 SecureSync/9400s:** (at least versions 5.2.1 and below are not affected by this vulnerability, as shown below)

OpenSSl last updated to:

- version 1.0.1M in V5.2.1 (not affected)
- v5.2.0 uses 1.0.1k. (not affected)
- v5.1.6 through 5.1.7 use 1.0.1i (not affected)
- v5.1.5 uses 1.0.1h (not affected)
- v5.1.4 uses 1.0.1g (not affected)
- v5.0.0 through 5.1.3 used 1.0.1e (not affected)

- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (v3.6.0 through v3.6.5 use OpenSSL 1.0.1C, and v3.6.6 uses OpenSSL1.0.1g)

CVE-2015-1792

- **Refer to**: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1792
- Refer to Mantis case 3059 for SecureSyncs and NetClock 9400s.
- **Description:** The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure
- OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b

Products:

- **1200 SecureSync/9400s:** OpenSSl last updated to version 1.0.1M in V5.2.1 (at least versions 5.2.1 and below are vulnerable)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable)

CVE-2015-1791

- **Refer to**: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1791
- Refer to Mantis case 3059 for SecureSyncs and NetClock 9400s.
- **Description**: Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash
- OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b,

Products:

- **1200 SecureSync/9400s:** OpenSSl last updated to version 1.0.1M in V5.2.1 (at least versions 5.2.1 and below are vulnerable)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable)

CVE-2015-1790

- **Refer to**: https://security-tracker.debian.org/tracker/CVE-2015-1790
- Refer to Mantis case 3059 for SecureSyncs and NetClock 9400s.
- **Description**: The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data.
- OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b

Products:

- **1200 SecureSync/9400s:** OpenSSl last updated to version 1.0.1M in V5.2.1 (at least versions 5.2.1 and below are vulnerable)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable)

CVE-2015-1789

- **Refer to**: https://security-tracker.debian.org/tracker/CVE-2015-1789
- Refer to Mantis case 3059 for SecureSyncs and NetClock 9400s.
- **Description**: The X509_cmp_time function in crypto/x509/x509_vfy. allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.
- OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b

Products:

- **1200 SecureSync/9400s:** OpenSSl last updated to version 1.0.1M in V5.2.1 (at least versions 5.2.1 and below are vulnerable)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable)

CVE-2015-1788

- **Refer to**: https://security-tracker.debian.org/tracker/CVE-2015-1788
- Refer to Mantis case 3059 for SecureSyncs and NetClock 9400s.
- **Description**: The BN_GF2m_mod_inv function in crypto/bn/bn_gf2m.c does not properly handle ECParameters structures in which the curve is over a malformed binary polynomial field, which allows remote attackers to cause a denial of service (infinite loop) via a session that uses an Elliptic Curve algorithm, as demonstrated by an attack against a server that supports client authentication.
- OpenSSL before 0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b

Products:

- **1200 SecureSync/9400s:** OpenSSl last updated to version 1.0.1M in V5.2.1 (at least versions 5.2.1 and below are vulnerable)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.

CVE-2014-3581 / CVE-2014-3583

- **Refer to**:
- **Description**:

Products:

- **VersaSyncs**
- **1232 VelaSyncs:**
- **1200 SecureSync/9400s:** Apache was updated to 2.4.41 in v5.9.0 update, resolving this vulnerability (refer to v5.9.0 Release Notes)
- **NetClock 9300 and 9200 series**: OpenSSl last updated to version 1.0.1j in V3.6.7 (at least versions 3.6.7 and below are vulnerable) Note there are no further software updates expected for these NTP servers.

CVE-2014-2830 (Stack-based buffer overflow in cifskey.c or cifscreds.c)

- Refer to https://nvd.nist.gov/vuln/detail/CVE-2014-2830

Stack-based buffer overflow in cifskey.c or cifscreds.c in cifs-utils before 6.4, as used in pam_cifscreds, allows remote attackers to have unspecified impact via unknown vectors.

Products:

- **Legacy VelaSync: ?**
- **1200 SecureSync/9400s:** versions 5.6.0 and below are affected (fixed in v5.7.0 update per JIRA ticket SSS-200)
- **NetClock 9300 and 9200 series**:?

CVE-2014-0076 (Montgomery ladder in OpenSSL)

➢ Refer to: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0076

The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack

- ○ Fixed in OpenSSL 1.0.1g (git commit) (Affected 1.0.1f, 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1)
- ○ Fixed in OpenSSL 1.0.0m (git commit) (Affected 1.0.0l, 1.0.0k, 1.0.0j, 1.0.0i, 1.0.0g, 1.0.0f, 1.0.0e, 1.0.0d, 1.0.0c, 1.0.0b, 1.0.0a, 1.0.0)
- ○ Fixed in OpenSSL 0.9.8za (Affected 0.9.8y, 0.9.8x, 0.9.8w, 0.9.8v, 0.9.8u, 0.9.8t, 0.9.8s, 0.9.8r, 0.9.8q, 0.9.8p, 0.9.8o, 0.9.8n, 0.9.8m, 0.9.8l, 0.9.8k, 0.9.8j, 0.9.8i, 0.9.8h, 0.9.8g, 0.9.8f, 0.9.8e, 0.9.8d, 0.9.8c, 0.9.8b, 0.9.8a, 0.9.8)

Products:

- ○ **Legacy VelaSync:**
- ○ **1200 SecureSync/9400s:**
- **NetClock 9300 and 9200 series**: Software versions 3.6.5 and below are affected (version 3.6.6 update OpenSSL to version 1.0.1g). Note there are no further software updates expected for these NTP servers.

Multiple CVEs associated with versions of PHP and other libraries

PHP, and other libraries:

• **PHP:** Multiple vulnerabilities (dev-lang/php-5.5.37 dev-lang/php-5.6.17) CVE-2013-6501,CVE-2014-9705,CVE-2014-9709,CVE-2015-0231,CVE-2015-0273,CVE-2015-1351,CVE-2015-1352,CVE-2015-2301,CVE-2015-2348,CVE-2015-2783,CVE-2015-2787,CVE-2015-3329,CVE-2015-3330,CVE-2015-4021,CVE-2015-4022,CVE-2015-4025,CVE-2015-4026,CVE-2015-4147,CVE-2015-4148,CVE-2015-4642,CVE-2015-4643,CVE-2015-4644,CVE-2015-6831,CVE-2015-6832,CVE-2015-6833,CVE-2015-6834,CVE-2015-6835,CVE-2015-6836,CVE-2015-6837,CVE-2015-6838,CVE-2015-7803,CVE-2015-7804, 201607-02 [N] [remote]

• :**Multiple Vulnerabilities** (dev-libs/libpcre-8.36) CVE-2014-8964,CVE-2014-8964,CVE-2015-5073,CVE-2015-5073,CVE-2015-5073,CVE-2015-8380,CVE-2015-8381,CVE-2015-8383,CVE-2015-8384,CVE-2015-8385,CVE-2015-8386,CVE-2015-8387,CVE-2015-8388,CVE-2015-8389,CVE-2015-8390,CVE-2015-8391,CVE-2015-8392,CVE-2015-8393,CVE-2015-8394,CVE-2015-8395,CVE-2016-1283,CVE-2016-1283, 201607-04 [N] [remote]

• **GD**: Multiple vulnerabilities (media-libs/gd-2.0.35-r4) CVE-2016-3074

Products:

- ○ **2400 SecureSyncs/VersaSyncs**

2400 **S/S Version**	**PHP version**
1.4.3	Updated to version 8.0.20
1.4.1	Version 7.4.15
1.2.1 and 1.2.2	Updated to **7.4.4**
1.2.0	? 5.6.35-pl1 ?

- ○ **Legacy VelaSyncs**

- **1200 SecureSyncs and 9400s: all of the above CVEs were fixed with the version 5.4.5 update (Sept 2016) with PHP and other libraries being updated to a newer version.**
- **NetClock 9300 and 9200 series NetClocks with versions 3.6.7 and below installed are affected.**

CVE-2012-6708 (jQuery vulnerability)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2012-6708

Description jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks.

Products:

- **2400 SecureSyncs and 9400s**
- **Legacy VelaSyncs**
- **1200 SecureSyncs and 9400s (at least versions 5.9.5 and below appear affected)**
  - Refer to Salesforce Cases such as 2700076, 287874
  - Refer to JIRA SSS-1178 (looking at fix in 5.9.6 towards beginning of 2023)

NetClock 9300 and 9200 series

CVE-2012-2141 Net-SNMP Denial of Service (Zero-Day)

- Refer to: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2141
- **Description:** Array index error in the handle_nsExtendOutput2Table function in agent/mibgroup/agent/extend.c in Net-SNMP 5.7.1 allows remote authenticated users to cause a denial of service (out-of-bounds read and snmpd crash) via an SNMP GET request for an entry not in the extension table.
- Net**-**SNMP versions 5.7.1 and below.

Products:

- **2400 SecureSyncs**
- **1200 SecureSyncs/9400s:** Software versions 5.3.0 and below (addressed in version 5.3.1, ~Dec 2015)
- **NetClock 9300 and 9200 series**: At least versions 3.6.7 and below (I believe, but this is not confirmed)

CVE-2010-5298

- Refer to https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-5298

Summary: Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.

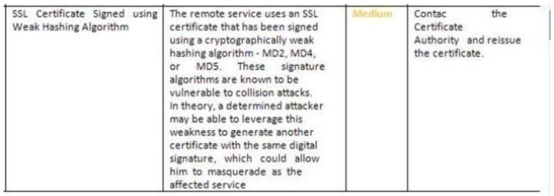
Fixed in OpenSSL version 1.0.1h and OpenSSL 1.0.0m

Products:

- **Legacy VelaSyncs**
- **1200 SecureSyncs**

- ○ **NetClock 9300 and 9200 series NetClocks with versions 3.6.6 and below installed are affected (fix is in version 3.6.7 and above. V3.6.7 updated OpenSSL to v1.01j)**

CVE-2004-2761 SSL Certificate Signed using Weak Hashing Algorithm



SSL Certificate Signed using Weak Hashing Algorithm	The remote service uses an SSL certificate that has been signed using a cryptographically weak hashing algorithm - MD2, MD4, or MD5. These signature algorithms are known to be vulnerable to collision attacks. In theory, a determined attacker may be able to leverage this weakness to generate another certificate with the same digital signature, which could allow him to masquerade as the affected service	Medium	Contac the Certificate Authority and reissue the certificate.

This reported vulnerability is indicating the MD5 authentication being used for the “Signature Algorithm” is not the most secure algorithm, as other stronger algorithms are available. As described above, if you choose to create a new self-signed certificate, you should select “SHA1” as the desired “Signature Algorithm” as SHA1 is now a stronger cipher than MD5.

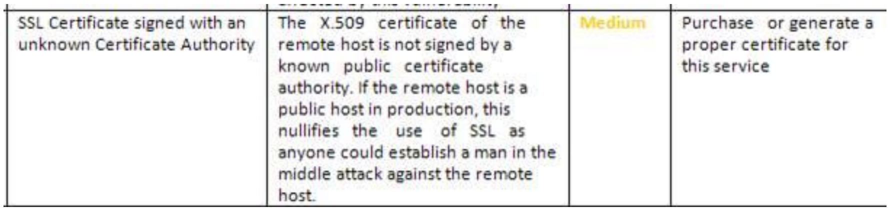
“SSL Certificate - Signature Verification Failed Vulnerability” (“port 443/tcp over SSL”)

- ➢ **Category**: General remote services
- ➢ No CVE ID assigned
- ➢ Found during a SecureSync version 5.5.0 scan

From https://devcentral.f5.com/questions/ssl-certificate-signature-verification-failed-vulnerability
I assume a basic vulnerability scan (probably with Qualys) was performed against the management interface of your BIG-IP?
In that case it probably doesn't like that you are using the the self signed BIG-IP server certificate which isn't signed by a CA the scanning tool knows. so to resolve this you have to put a certificate signed by a known CA on the BIG-IP:
http://support.f5.com/kb/en-us/solutions/public/14000/600/sol14620.html

----

“SSL Certificate signed with an unknown Certificate Authority”



SSL Certificate signed with an unknown Certificate Authority	The X.509 certificate of the remote host is not signed by a known public certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man in the middle attack against the remote host.	Medium	Purchase or generate a proper certificate for this service

Spectracom provides a default HTTPS certificate to alleviate the need to always purchase a certificate from an outside Certificate Authority (CA). This report is recommending that you do not use the Spectracom certificate. To prevent this report, you will need to either use your own internal Certificate Authority (CA), if available, or you will need to purchase one from an external Certificate Authority (CA) such as Verisign or godaddy.com.

CVE-2004-0790

- Refer to https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0790 and http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-0790

Summary: Multiple TCP/IP and ICMP implementations allow remote attackers to cause a denial of service (reset TCP connections) via spoofed ICMP error messages, aka the "blind connection-reset attack

Products:

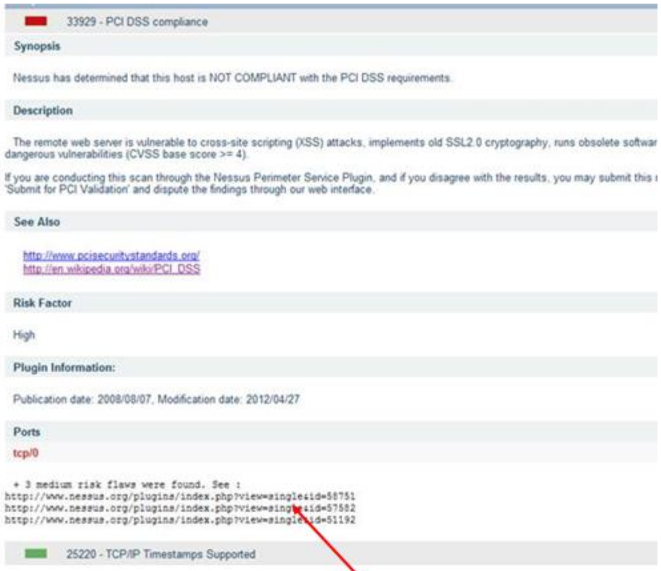
- **SecureSyncs**
- **NetClock 9300 and 9200 series**

PCI DSS compliance (Payment Card Industry)

- Refer also to “PCI DSS” in the SecureSync Cust Assistance document

A vulnerability scanner can detect/report PCI DSS Compliancy

This report is not an individual report of a potential vulnerability being detected. It’s reporting that the device is not PCI DSS compliant, because there are reports of potential vulnerabilities that are being detected. The unresolved/detected potential vulnerabilities are listed at the bottom of the report (under “Ports”, as shown in the example below):



🟥 33929 - PCI DSS compliance

Synopsis

Nessus has determined that this host is NOT COMPLIANT with the PCI DSS requirements.

Description

The remote web server is vulnerable to cross-site scripting (XSS) attacks, implements old SSL2.0 cryptography, runs obsolete softwar dangerous vulnerabilities (CVSS base score >= 4).

If you are conducting this scan through the Nessus Perimeter Service Plugin, and if you disagree with the results, you may submit this 'Submit for PCI Validation' and dispute the findings through our web interface.

See Also

http://www.pcisecuritystandards.org/
http://en.wikipedia.org/wiki/PCI_DSS

Risk Factor

High

Plugin Information:

Publication date: 2008/08/07, Modification date: 2012/04/27

Ports

tcp/0

```
 + 3 medium risk flaws were found. See :
http://www.nessus.org/plugins/index.php?view=single&id=58751
http://www.nessus.org/plugins/index.php?view=single&id=57582
http://www.nessus.org/plugins/index.php?view=single&id=51192
```

🟩 25220 - TCP/IP Timestamps Supported

In this example, items 58751, 57582 and 51192 are detected potential vulnerabilies. Clearing these items will allow this report to be automatically cleared

In this example, items 58751, 57582 and 51192 are detected potential vulnerabilies. Clearing these items will allow this report to be automatically cleared

----

FTP being enabled

- **Condition/cause**: FTP port is enabled
- **Fix:** disable the “unsecure” FTP service. Consider using SFTP/SCP instead.

Example reports associated to FTP being enabled:

A) “FTP - Allows clear text authentication without encryption”

B) “FTP Server detected”

Telnet being enabled

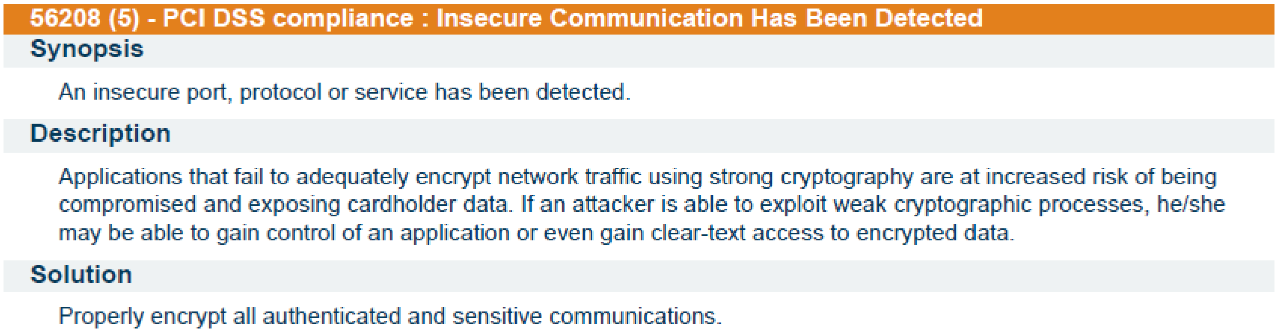
- **Condition/cause**: Telnet port is enabled (Telnet uses TCP port 23)
- **Fix:** disable the “unsecure” Telnet service

Example reports associated to telnet service being enabled:

A) “Telnet server transmits unencrypted Traffic”

B) “Telnet – Clear Text Transmission Password /User Name”

C) “PCI DSS Compliance: Insecure Communication Has Been Detected (telnet)”



56208 (5) - PCI DSS compliance : Insecure Communication Has Been Detected

Synopsis

An insecure port, protocol or service has been detected.

Description

Applications that fail to adequately encrypt network traffic using strong cryptography are at increased risk of being compromised and exposing cardholder data. If an attacker is able to exploit weak cryptographic processes, he/she may be able to gain control of an application or even gain clear-text access to encrypted data.

Solution

Properly encrypt all authenticated and sensitive communications.

Keith’s response (10/16/12): Services such as telnet, FTP and HTTP are unsecure connections by design. All Services in the NetClock can be Enabled/Disabled as desired. For security reasons, we recommend customers disable all unsecure services such as telnet, HTTP and FTP. Services can be enabled or disabled in the **Network** -> **General** Setup page of the browser, **Services** tab. By default all services, besides Daytime and Time, are enabled.

I recommend your customer disable the Telnet, FTP and HTTP Services in this tab and then rescan the NetClock. This potential vulnerability should no longer occur.

OpenSSH

- **Fix:** Update software to the latest version to have latest OpenSSH rev installed

Example scan reports related to OpenSSH

A) "OpenSSH <=6.6 SFTP misconfiguration exploit for 64bit Linux – Remote"

Reference: http://seclists.org/fulldisclosure/2014/Oct/35

Fix: (Upgrade OpenSSH to version 6.7 or higher)

- ○ **2400 SecureSyncs/VersaSyncs**:
- ○ **1200 SecureSyncs/9400s**: OpenSSH last updated to version 6.6p1 in V5.1.7 (at least 5.1.7 and below are still vulnerable)
- ○ **NetClock 9300/9200**: OpenSSH last updated to version 6.6p1 in V3.6.6 (at least 3.6.7 and below are still vulnerable)

B) SSH Local Access Not Available

- **Cause:** the scanner was unable to login to the remote system via SSH
- OpenSSH may be disabled in services. Login credentials may be incorrect

----

Web browser (HTTP/HTTPS)

Example scan reports

A) "Web Resource /.cgi-bin/loigin_adv.tcl Detected"

Details: The presence of the URI 'cgi-bin/loginadv.tcl' has been discovered on the web server. This resource could potentially lead to brute force attacks and if successful could lead sensitive information disclosure and modification of configuration settings. Remove or restrict access to the detected web resource to deter potential exploitation:

Fix:

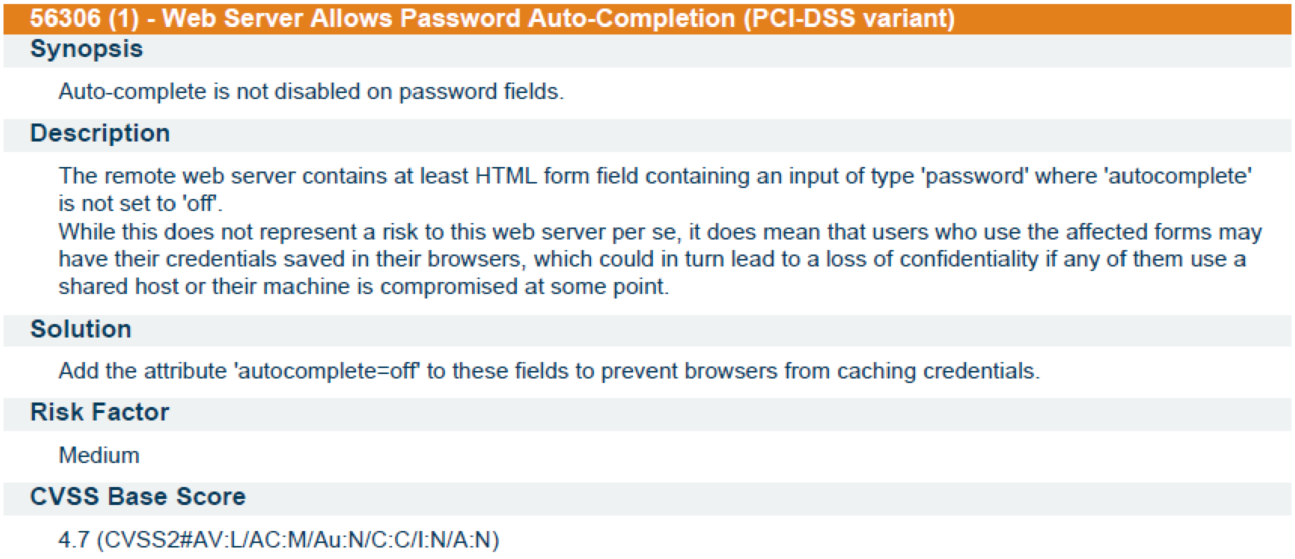
- ○ **2400 SecureSyncs/9400s**
  - ○ **1200 SecureSync/9400s**: Disable the "classic interface" web browser
    Note: Ability to disable the Classic interface was added in software version 5.1.4.
  - ○ **9300/9200**: "Upgrade to 1200 SecureSync/9400"

B) Directly related to HTTP being enabled

"HTTP 1.1 Protocol Detected"
"HTTP Server Cookies detected"

Condition/cause: "Unsecure" HTTP is enabled
Fix: Disable the "unsecure" HTTP service in Services

C) Web Server Allows Password Auto-Completion (PCI-DSS variant)



56306 (1) - Web Server Allows Password Auto-Completion (PCI-DSS variant)

Synopsis

Auto-complete is not disabled on password fields.

Description

The remote web server contains at least HTML form field containing an input of type 'password' where 'autocomplete' is not set to 'off'.
While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

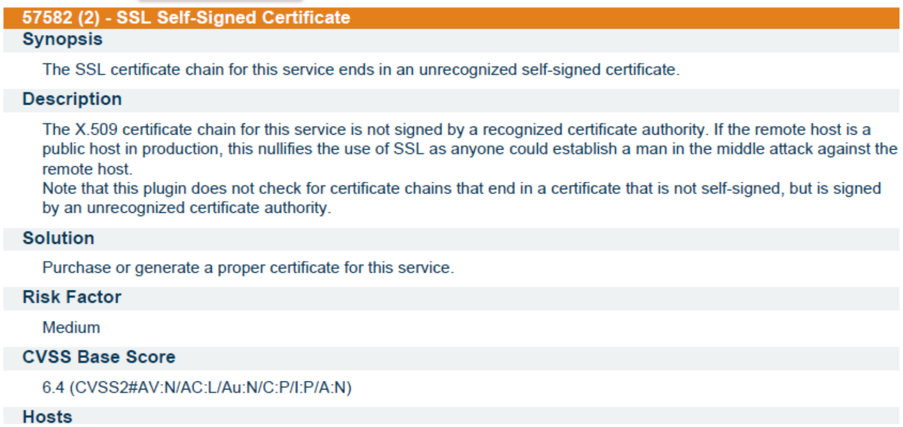
Medium

CVSS Base Score

4.7 (CVSS2#AV:L/AC:M/Au:N/C:C/I:N/A:N)

Keith's response (10/16/12): I believe we likely disable Password Auto-Completion. I will need to confirm this with Engineering.

- SSL Self-Signed Certificate and
- SSL Certificate Cannot Be Trusted and
- SSL Certificate Cannot Be Trusted



57582 (2) - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man in the middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

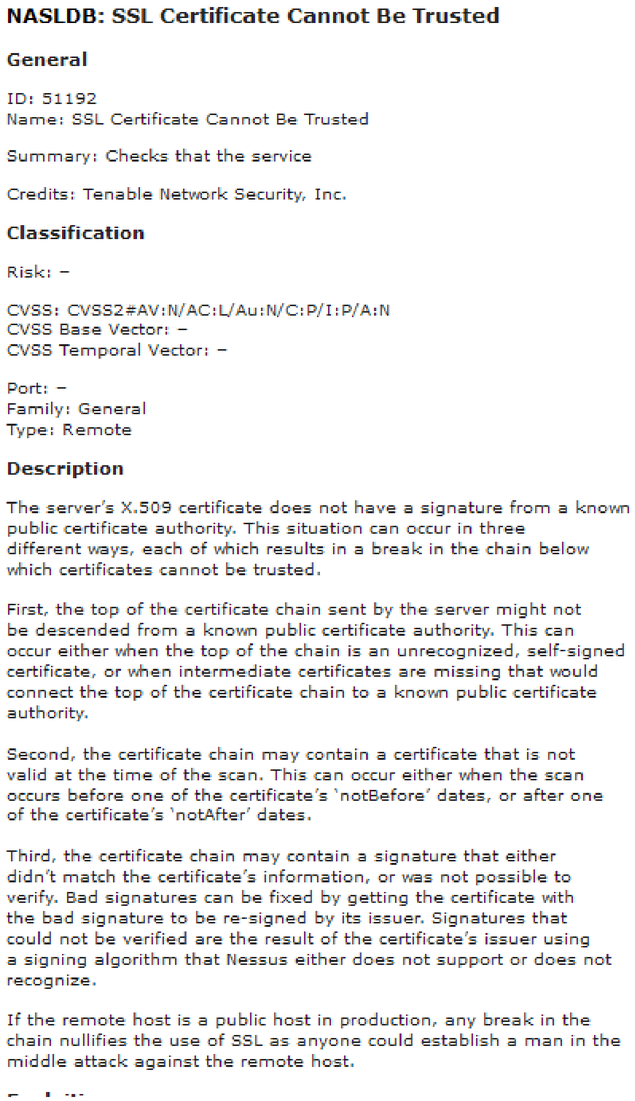
Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Hosts



NASLDB: SSL Certificate Cannot Be Trusted

General

ID: 51192
Name: SSL Certificate Cannot Be Trusted

Summary: Checks that the service

Credits: Tenable Network Security, Inc.

Classification

Risk: –

CVSS: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N
CVSS Base Vector: –
CVSS Temporal Vector: –

Port: –
Family: General
Type: Remote

Description

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

Third, the certificate chain may contain a signature that either didn't match the certificate's information, or was not possible to verify. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain nullifies the use of SSL as anyone could establish a man in the middle attack against the remote host.

Keith's response (10/16/12): A customer can either use the factory default Spectracom self-signed Certificate, or they can generate their own certificate. Attached is a document that discusses how to replace the default certificate with their own certificate. This consists of generating a Certificate Request in the NetClock and then exporting this CR for a new Certificate to be generated. Then, the new certificate can be inserted into the SecureSync.

Disable TLS/SSL support for static key cipher suites
TLS/SSL Server Supports the Use of Static Key Ciphers

Recommendation: Disable TLS/SSL support for static key cipher suites.
Configure the server to disable support for static key cipher suites. For Microsoft IIS web servers, see Microsoft Knowledgebase article 245030 (http://support.microsoft.com/kb/245030/) for instructions on disabling static key cipher suites. The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.Refer to your server vendor documentation to apply the recommended cipher configuration:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-

RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

TLS Server Supports TLS version 1.0
The PCI (Payment Card Industry) Data Security Standard requires a minimum of TLS v1.1 and recommends TLS v1.2. In addition, FIPS 140-2 standard requires a minimum of TLS v1.1 and recommends TLS v1.2.

Recommendation: Disable insecure TLS/SSL protocol support. Configure the server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.

TLS Server Supports TLS version 1.1
The PCI (Payment Card Industry) Data Security Standard requires a minimum of TLS v1.1 and recommends TLS v1.2. In addition, FIPS 140-2 standard requires a minimum of TLS v1.1 and recommends TLS v1.2.

Recommendation: Disable insecure TLS/SSL protocol support. Configure the server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.

There were two other findings, but I think those were fixed when I applied the corporately signed certificate.

CVE-2004-0079 (do_change_cipher_spec)

Refer to sites such as: https://www.saucs.com/cve/CVE-2004-0079

Summary: The do_change_cipher_spec function in OpenSSL 0.9.6c to 0.9.6k, and 0.9.7a to 0.9.7c, allows remote attackers to cause a denial of service (crash) via a crafted SSL/TLS handshake that triggers a null dereference.

Products:

- ○ **Prisma VelaSyncs**
- ○ **Legacy VelaSyncs**
- ○ **1200 SecureSyncs: at least versions 4.8.9 and above use openSSL versions 1.x (beyond 0.9.x) and so are not affected.**
- ○ **NetClock 9300 and 9200 series NetClocks with versions 3.6.7 and below installed are affected??**

CVE-1999-0524 “ICMP TimeStamp Request”

Refer to: **http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0524**

Issue: ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts.

Fix: Filter or block ICMP (Type 13) requests on the target using a host-based firewall or endpoint protection software

----

"TCP Sequence Number Approximation Based Denial of Service" ([NISCC Vulnerability Advisory 236929]**)**

- Refer to Salesforce Case 284824/ JIRA ticket SSS-1287 (12 July 2022).
- Reported as detected in SecureSync with v5.9.1 installed (may be a false positive)
- Refer to https://dl.packetstormsecurity.net/0404-advisories/246929.html
  - References **CVE-2004-0230 (**https://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0230)
  - See much earlier info directly below:

CVE-2004-0790, CVE-2004-0791, and CVE-2004-1060 CVE-2005-0065, CVE-2005-0066, CVE-2005-0067, and CVE-2005-0068

- **Related CVE's**: CVE-2004-0790, CVE-2004-0791, and CVE-2004-1060, CVE-2005-0065, CVE-2005-0066, CVE-2005-0067, and CVE-2005-0068
- Refer to Mantis case 2392 and Fogbugz case 1857
- **Refer to Salesforce Case 11892** (https://na8.salesforce.com/500C000000U06MF) for a good response.

Per Paul Myers (7 Oct 2013): Added as FogBugz case 1857 and Mantis case 2392 RESOLVED BOTH AS DO NOT FIX.

These CVE-2004-0230 and CVE-2004-0790 appear to be implementation issues common to TCP based operating systems IP stacks.

RedHat, Debian, and the general linux community have graded these risks as overstated and have not moved to resolve these as they are derived from the implementation of TCP.

These also may be considered FALSE positives because we might not actually be exploitable or the situation the customer is in may not even be exploitable! The typical worst case is a reset of a TCP web page connection. This will not interfere with operation of the NetClock. Also, if their network infrastructure is so badly compromised they have far worse concerns.

Our box is primarily a UDP NTP Server. TCP connections such as web access should be INFREQUENT and for their applications they should reside in private/secure networks. Insecure protocols should be disabled. There is no risk to timekeeping or NTP access to the NetClock.

Related CVE's

CVE-2004-0790, CVE-2004-0791, and CVE-2004-1060, CVE-2005-0065, CVE-2005-0066, CVE-2005-0067, and CVE-2005-0068

REDHAT RESPONSE
The DHS advisory is a good source of background information about the issue: http://www.us-cert.gov/cas/techalerts/TA04-111A.html It is important to note that the issue described is a known function of TCP**. In order to perform a connection reset an attacker would need to know the source and destination ip address and ports as well as being able to guess the sequence number within the window. These requirements seriously reduce the ability to trigger a connection reset on normal TCP connections.** The DHS advisory explains that BGP routing is a specific case where being able to trigger a reset is easier than expected as the end points can be easily determined and large window sizes are used. BGP routing is also significantly affected by having it's connections terminated. The major BGP peers have recently switched to requiring md5 signatures which mitigates against this attack. The following article from Linux Weekly News also puts the flaw into context and shows why it does not pose a significant threat: http://lwn.net/Articles/81560/ Red Hat does not have any plans for action regarding this issue.
Source: Redhat

Debian Response
https://security-tracker.debian.org/tracker/CVE-2004-0230

"The attack works with a certain non-negligible probability, but even when successful, it only causes a TCP disconnect, which will (in most circumstances) be reestablished right away, causing essentially no impact"

CVE-2004-0230 (TCP)

- Refer to:

  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0230

  https://success.qualys.com/discussions/s/question/0D52L00004TnvT9SAJ/cve20040230-tcp-sequence-number-approximation-based-denial-of-service

Description: *per CVE-2004-0230 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-0230)*

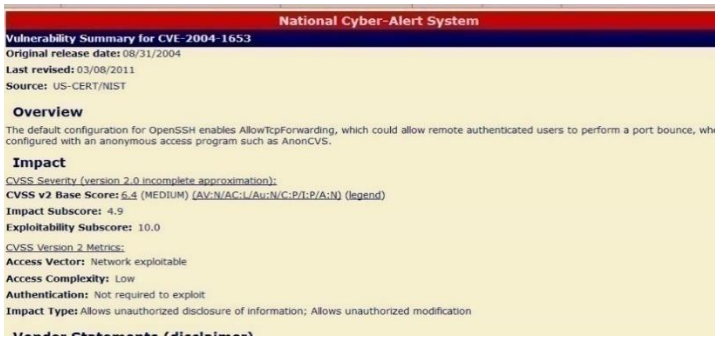
TCP, when using a large Window Size, makes it easier for remote attackers to guess sequence numbers and cause a denial of service (connection loss) to persistent TCP connections by repeatedly injecting a TCP RST packet, especially in protocols that use long-lived connections, such as BGP

CVE-2004-0790 (TCP)

CVE-2004-0790 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-0790)
- Multiple TCP/IP and ICMP implementations allow remote attackers to cause a denial of service (reset TCP connections) via spoofed ICMP error messages, aka the "blind connection-reset attack." NOTE: CVE-2004-0790, CVE-2004-0791, and CVE-2004-1060 have been SPLIT based on different attacks; CVE-2005-0065, CVE-2005-0066, CVE-2005-0067, and CVE-2005-0068 are related identifiers that are SPLIT based on the underlying vulnerability. While CVE normally SPLITs based on vulnerability, the attack-based identifiers exist due to the variety and number of affected implementations and solutions that address the attacks instead of the underlying vulnerabilities.

CVE-2004-1653 (“OpenSSH >= 2.3.0 AllowTcpForwarding Port Bouncing”)

- Refer to Salesforce case 12684 (https://na8.salesforce.com/500C000000VLuyW)
- Reported in SecureSync version 4.8.8
- Refer to sites such as https://www.tenable.com/plugins



National Cyber-Alert System

Vulnerability Summary for CVE-2004-1653

Original release date: 08/31/2004

Last revised: 03/08/2011

Source: US-CERT/NIST

Overview

The default configuration for OpenSSH enables AllowTcpForwarding, which could allow remote authenticated users to perform a port bounce, whe configured with an anonymous access program such as AnonCVS.

Impact

CVSS Severity (version 2.0 incomplete approximation):

CVSS v2 Base Score: 6.4 (MEDIUM) (AV:N/AC:L/Au:N/C:P/I:P/A:N) (legend)

Impact Subscore: 4.9

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification

Vendor Statements (disclaimer)

Keith’s response: This appears to be related to SSH versions prior to version 3.9. 1200 SecureSync/9400s with software versions 4.8.0 and above are running **SSH version 5.9p1**, so this potential vulnerability is not applicable to the SecureSyncs/9400s with versions 4.8.1 and above installed

----

CVE 2004-2004

CVE 2004-2761 (MD5 Message-Digest Algorithm is not collision resistant)

Refer to http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2761 and https://nvd.nist.gov/vuln/detail/CVE-2004-2761

The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5 in the signature algorithm of an X.509 certificate.

Email from Dave Lorah (SF Case 169299, 12 July 2018) pertaining to SecureSyncs/9400s: I have some information on the CVE-2004-2761 Vulnerability.

"The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5 in the signature algorithm of an X.509 certificate."

This cannot be fixed by a firmware update.

This reported vulnerability is indicating the MD5 authentication being used for the "Signature Algorithm" is not the most secure algorithm, as other stronger algorithms are available. If you choose to create a new self-signed certificate, you should select "SHA1" as the desired "Signature Algorithm" as SHA1 is now a stronger cipher than MD5.

The SecureSync uses MD5 for its default SSH certificate. The reported "potential vulnerability" indicates that MD5 is only a medium strength cipher and that better ciphers are available. In order to use a better cipher, you can manually delete the default self-signed Spectracom HTTPS certificate and concurrently create your own certificate instead, using better SHA1 or SHA256 as an alternate cipher to MD5.

Severity

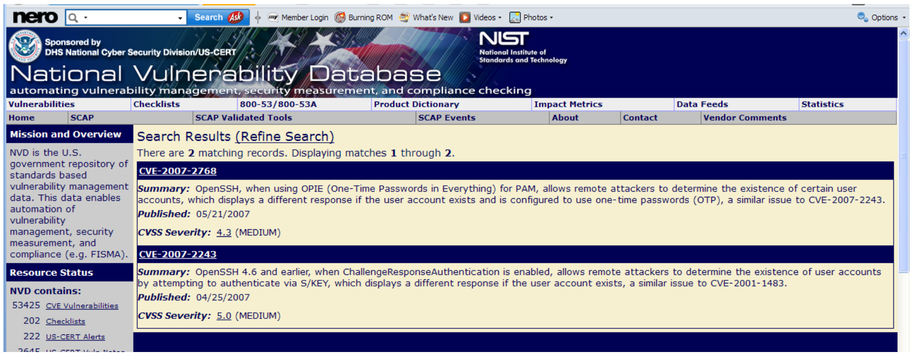
Products:

- ○ **1232 VelaSyncs**
- ○ **Legacy VelaSyncs:**
- ○ **1200 SecureSync**: is version 5.x. They are N/A because it at a version that was fixed and because we don't support X connections in our time servers.
- ○ **NetClocks (9300 and 9200 series): ?**

CVE-2007-2243 and CVE-2007-2768 “OpenSSH S/KEY Authentication Account Enumeration” and

“OPIE w/ OpenSSH Account Enumeration”

- (OTP= One Time Passwords)
- Per Ron Dries (14 July 2020) “… I did ask Engineering and we it looks like we don’t use OPIE or OTP pam modules.



Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

53425	CVE Vulnerabilities
202	Checklists
222	US-CERT Alerts

Search Results (Refine Search)

There are **2** matching records. Displaying matches **1** through **2**.

CVE-2007-2768

Summary: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

Published: 05/21/2007

CVSS Severity: 4.3 (MEDIUM)

CVE-2007-2243

Summary: OpenSSH 4.6 and earlier, when ChallengeResponseAuthentication is enabled, allows remote attackers to determine the existence of user accounts by attempting to authenticate via S/KEY, which displays a different response if the user account exists, a similar issue to CVE-2001-1483.

Published: 04/25/2007

CVSS Severity: 5.0 (MEDIUM)

Keith’s response (10/16/12): This appears to be related to SSH versions prior to version 4.6. NetClocks with Archive software versions 4.8.0 and above are running SSH version 5.9p1 so this potential vulnerability is not applicable to the NetClock.

More recent info

Email from Ron Dries (14 July 2020) Hi Keith and Dave,

So, they don’t specify a specific CVE. So, we won’t know if it is specific to certain openSSH versions.

However. I did ask Engineering and we it looks like we don’t use OPIE or OTP pam modules.

CVE-2007-2243 and CVE-2008-1483 OpenSSH

Vulnerability Summary for CVE-2008-1483 (This issue was reported to us on 5/12/10)
Original release date:03/24/2008
Last revised:12/28/2009
Source: US-CERT/NIST
Overview
OpenSSH 4.3p2, and probably other versions, allows local users to hijack forwarded X connections by causing ssh to set DISPLAY to :10, even when another process is listening on the associated port, as demonstrated by opening TCP port 6010 (IPv4) and sniffing a cookie sent by Emacs.
Impact
CVSS Severity (version 2.0):
CVSS v2 Base Score:6.9 (MEDIUM) (AV:L/AC:M/Au:N/C:C/I:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 3.4
CVSS Version 2 Metrics:
Access Vector: Locally exploitable
Access Complexity: Medium
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

Summary: OpenSSH 4.3p2, and probably other versions, allows local users to hijack forwarded X connections by causing ssh to set DISPLAY to :10, even when another process is listening on the associated port, as demonstrated by opening TCP port 6010 (IPv4) and sniffing a cookie sent by Emacs.

Fix: This issue appears to be resolved in SSH version 5.

Severity

Products:

- ○ **SecureSync**: is version 5.x. They are N/A because it at a version that was fixed and because we don't support X connections in our time servers.

- ○ **NetClocks (9300 and 9200 series): NetClocks are version 4.7. They are N/A because we don't support X connections in our time servers.**

CVE-2008-1483 (OpenSSH X11 Forwarding Information Disclosure Vulnerability)

- ➢ OpenSSH versions prior to versions 6.6 are vulnerable

Severity

Products:

- ○ **SecureSyncs**

- ○ **NetClock 9300 and 9200 series**

  SSH was upgraded to 6.6p1 in the version 3.6.6 Software update. So the answer it is mitigated with the version 3.6.6 update.

CVE-2008-3259 (OpenSSH "X11UseLocalhost" X11 Forwarding Session Hijacking Vulnerability)

- OpenSSH versions prior to versions 5.1 are vulnerable.

Severity

Products:

- **SecureSyncs**
- **NetClock 9300 and 9200 series**

  The mitigation is to “Upgrade to OpenSSH version 5.1”. SSH was upgraded to 6.6p1 in the version 3.6.6 software update. So the answer it is mitigated with the version 3.6.6 update.

CVE-2008-5161 (OpenSSH CBC Mode vulnerability)

- Refer to http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5161

Description: Error handling in the SSH protocol in (1) SSH Tectia Client and Server and Connector 4.0 through 4.4.11, 5.0 through 5.2.4, and 5.3 through 5.3.8; Client and Server and ConnectSecure 6.0 through 6.0.4; Server for Linux on IBM System z 6.0.4; Server for IBM z/OS 5.5.1 and earlier, 6.0.0, and 6.0.1; and Client 4.0-J through 4.3.3-J and 4.0-K through 4.3.10-K; and (2) OpenSSH 4.7p1 and possibly other versions, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors.

- This is n order to mitigate this vulnerabilty SSH can be setup to use CTR mode rather CBC mode. According to CPNI Vulnerability Advisory SSH:
- The most straightforward solution is to use CTR mode instead of CBC mode, since this renders SSH resistant to the attack. An RFC already exists to standardise counter mode for use in SSH (RFC 4344) ...sue was addressed for Red Hat Enterprise Linux 5

Severity

Susceptible versions: OpenSSH versions prior to versions 5.2 and 5.2p1 are vulnerable.

Products:

- **SecureSync Mitigated in Archive version 4.8.0 (if not earlier). V4.8.0 added OpenSSH 5.9.**

  Archive version 5.0.2 is at OpenSSH 6.1p1.

- **NetClock 9300 and 9200 series SSH was upgraded to 6.6p1 in the version 3.6.6 Software update. So, the answer is it is mitigated with the version 3.6.6 update.**

- **SecureSync CLI command to verify SSH version**: **version ssh** (reports SSL version on top row and SSH version in 2nd row).

Reply from Paul Myers (27 Jan 2014)
We are at openSSH 6.1p1
This affects OpenSSH 4.7p1, I don't see where it affects our version.

From http://www.securityfocus.com/bid/32319

Not vulnerable (Note: SecureSync OpenSSH updated to 5.9p1 in Archive version 4.8.0)
OpenSSH OpenSSH 5.2p1
OpenSSH OpenSSH 5.2

Vulnerable
OpenSSH OpenSSH 4.2
OpenSSH OpenSSH 4.1 p1
OpenSSH OpenSSH 4.1
OpenSSH OpenSSH 4.0 p1
OpenSSH OpenSSH 4.0
OpenSSH OpenSSH 5.1
OpenSSH OpenSSH 5.0
OpenSSH OpenSSH 4.9
OpenSSH OpenSSH 4.8
OpenSSH OpenSSH 4.7p1
OpenSSH OpenSSH 4.7
OpenSSH OpenSSH 4.6p1
OpenSSH OpenSSH 4.6
OpenSSH OpenSSH 4.5
OpenSSH OpenSSH 4.4.p1
OpenSSH OpenSSH 4.4
OpenSSH OpenSSH 4.3p2
OpenSSH OpenSSH 4.3p1
OpenSSH OpenSSH 4.2p1

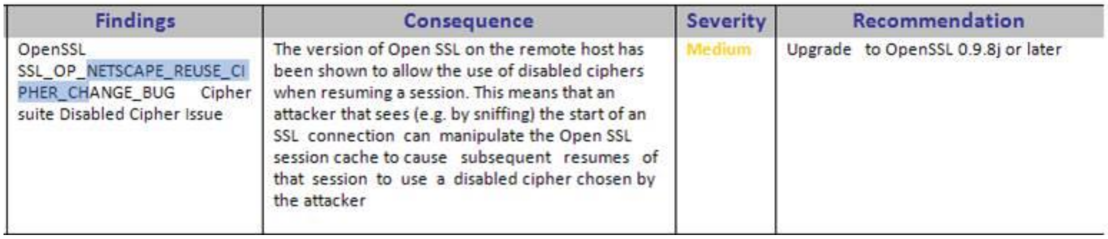
CVE-2008-7270 (SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled)

- Refer to: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7270
- Refer to Fogbugz case 1784 CVE number 2008-7270
- OpenSSL before 0.9.8j, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the use of a disabled cipher via vectors involving sniffing network traffic to discover a session identifier, a different vulnerability than CVE-2010-4180.
- Fix: Update OpenSSL to versions 0.9.8j or higher

Note: resolved with an upgrade to version 3.4.5 software. The SSL version in 3.4.5 does not implement a new version of SSL software. So, these vulnerabilities will still be detected.

Update: version 3.6.0 updated OpenSSL to version 1.0.1c so scanners just reading the version of OpenSSL will no longer report this vulnerability exists.

OpenSSL SSL_OP_NETSCAPE_REUSE_CI PHER_CHANGE_BUG Cipher suite Disabled Cipher Issue



Findings	Consequence	Severity	Recommendation
OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Cipher suite Disabled Cipher Issue	The version of Open SSL on the remote host has been shown to allow the use of disabled ciphers when resuming a session. This means that an attacker that sees (e.g. by sniffing) the start of an SSL connection can manipulate the Open SSL session cache to cause subsequent resumes of that session to use a disabled cipher chosen by the attacker	Medium	Upgrade to OpenSSL 0.9.8j or later

This is the first we have heard of this vulnerability being detected in the NetClock. It appears to be a medium level vulnerability. I am forwarding this report to our engineering team for their review. This vulnerability will likely require a NetClock software update to be made available in the future, in order to update to a newer version of SSL.

Severity

Products:

- **SecureSyncs/9400s**
  At least software update version 4.8.0 (Dec 2011), if not earlier, fixed this issue. Version 4.8.0 updated OpenSSL to version 1.0.0e. So, if the software is currently version 4.8.0 or higher, it's not susceptible. Earlier versions of our software may or may not be susceptible (more research would be needed to see if any earlier versions had an Open

- **NetClock 9300s**

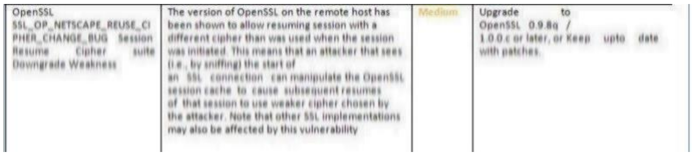
The following vulnerability was reported by Silvio Macias in a Model 9389 with version 3.4.3 installed (8/18/11)

CVE-2010-4180

- Refer to Fogbugz case 1784
- Refer to: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4180

The following vulnerability was reported by Silvio Macias in a Model 9389 with version 3.4.3 installed (8/18/11)

Note: resolved with an upgrade to version 3.4.5 software. The SSL version in 3.4.5 does not implement a new version of SSL software. So these vulnerabilities will still be detected.
OpenSSL SSL_OP_NETSCAPE_REUSE_CI PHER_CHANGE_BUG Session Resume Cipher suite Downgrade Weakness



OpenSSL SSL_OP_NETSCAPE_REUSE_CI PHER_CHANGE_BUG Session Resume Cipher suite Downgrade Weakness	The version of OpenSSL on the remote host has been shown to allow resuming session with a different cipher than was used when the session was initiated. This means that an attacker that sees (i.e., by sniffing) the start of an SSL connection can manipulate the OpenSSL session cache to cause subsequent resumes of that session to use weaker cipher chosen by the attacker. Note that other SSL implementations may also be affected by this vulnerability	Medium	Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or Keep upto date with patches.

This is the first we have heard of this vulnerability being detected in the NetClock. It also appears to be a medium level vulnerability. I am forwarding this report to our engineering team for their review. This vulnerability will also likely require a NetClock software update to be made available in the future, in order to update to a newer version of SSL.

Severity

CVE-2010-5107

- Refer to http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-5107
- Refer to Salesforce cases 12684 and 13129.
- Refer to Mantis case 2606 (http://cvsmantis.int.orolia.com/mantis/view.php?id=2606)
- Found in SecureSync 4.8.8
- Exists in at least Archive software versions 5.1.2 and below (not adding this to version 5.1.3 w/new browser,)
- Issue is with openSSH versions 6.1 and below. Need to update OpenSSH to version 6.2 to completely mitigate.
- Archive 5.1.2 is adding changes to the SSHD configuration to help mitigate this, until we have a chance to update OPenSSH to 6.2 in a future release.

Description The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.

Severity

Note: SecureSync CLI command to verify SSH version: **version ssh** (reports SSL version on top row and SSH version in 2nd row).

Email from Paul Myers, 18 Jan (5.0.2 still released, 5.1.2 in the works)
Keith – I updated the SSHD Configuration of SecureSync to allow MaxStartups 3:30:10
NOT MaxStartups 10:30:100
We support 3 logins up to 10, with the probability of logging in at 30% 4, and decreasing by 10% up to 10.
I don't think we need 10 logins for ssh and up to 100 logins.
Until OpenSSH is upgraded this is an improvement.
If they provide remote access we could make the change.

Email from Keith to David Dethefsen (28 Jan 2014, prior to v5.1.2 release)
Completely mitigating this potential condition requires updating openSSH from the current version 6.1 to the new version of 6.2. We are in the final stages of releasing a new SecureSync software update (version 5.1.2, more on this further below). We won't have time to incorporate this new version of OpenSSH in this pending release. However, as an improvement for this condition, until we can update Open SSH to version 6.2, we have modified the SSHD configurations to allow MaxStartups 3:30:10 (instead of 10:30:100). We will support 3 logins up to 10, with the probability of logging in at 30% 4, and decreasing by 10% up to 10.

I don't know when the OpenSSH update to version 6.2 will be made available. However, I have flagged your record to let you know when version 5.1.2 has been released to apply the changes to the SSHD configuration changes, as well as when a post version 5.1.2 update implements OpenSSH version 6.2 (note that we typically release a new version of software about once a quarter).

CVE-2011-3192 (Denial of Service attack)

- **Refer to:** http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3192

Summary: "The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlacpping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086."

Fix: Upgrade Apache to version 2.2.20.
Risk:

Severity

Products:

- **1200 SecureSync:**

  SecureSyncs with v4.8.0 software and below installed. Note that Apache was updated to software version 2.2.21 in version 4.8.0. This update should prevent this vulnerability (Mark Goodlein found that Apache software version 2.2.20 addresses this one).

- **NetClock 9300 and 9200 series:**

  Apache software hasn't been updated in quite a while (Apache is still at version 2.2.6 for versions of at least 3.4.5 through 3.4.8- likely also 3.4.4/3.4.3 but not confirmed). NetClock versions of at least 3.4.8 and below are susceptible to this potential vulnerability. Apache will need to be updated in a post 3.4.8 update to address this vulnerability.

  Status Update: Apache was updated in NetClocks to version 2.2.22 in Application software version 3.6.0.

CVE-2011-3389 httpd: cookie exposure due to error responses (AKA “Beast” Attack)

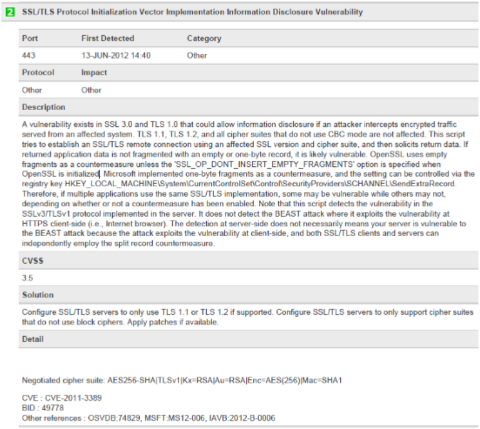
- Refer to sites such as:

http://resources.infosecinstitute.com/beast-vs-crime-attack/
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3389

Summary: The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.

Severity

SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability



2 **SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability**

Port	First Detected	Category
443	13-JUN-2012 14:40	Other
Protocol	**Impact**	
Other	Other	

Description

A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted traffic served from an affected system. TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected. This script tries to establish an SSL/TLS remote connection using an affected SSL version and cipher suite, and then solicits return data. If returned application data is not fragmented with an empty or one-byte record, it is likely vulnerable. OpenSSL uses empty fragments as a countermeasure unless the 'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when OpenSSL is initialized. Microsoft implemented one-byte fragments as a countermeasure, and the setting can be controlled via the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\SendExtraRecord. Therefore, if multiple applications use the same SSL/TLS implementation, some may be vulnerable while others may not, depending on whether or not a countermeasure has been enabled. Note that this script detects the vulnerability in the SSLv3/TLSv1 protocol implemented in the server. It does not detect the BEAST attack where it exploits the vulnerability at HTTPS client-side (i.e., Internet browser). The detection at server-side does not necessarily means your server is vulnerable to the BEAST attack because the attack exploits the vulnerability at client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure.

CVSS

3.5

Solution

Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported. Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available.

Detail

Negotiated cipher suite: AES256-SHA|TLSv1|Kx=RSA|Au=RSA|Enc=AES(256)|Mac=SHA1

CVE : CVE-2011-3389
BID : 49778
Other references : OSVDB:74829, MSFT:MS12-006, IAVB:2012-B-0006

Severity

Products:

- **SecureSyncs:**
- **NetClocks (9300 and 9200 series):**

No software updates associated with this CVE

Note from Paul Myers (10 Jan 2012) This potential vulnerability applies to SSL 3.0 and TLS 1.0. As indicated in the report: **The detection at server-side does not necessarily mean your server is vulnerable** to the BEAST attack because the attack exploits the vulnerability at client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure."

Note that we mitigate this attack by using RC4-SHA CipherSuites in a manner similar to what it suggested (from the excerpt below). Your scanner is not testing and finding this condition. It is merely detecting it because of the version information that it sees. No additional mitigation or action is required.

Below is detailed information for this report

- **from:** http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2008784)

Cause

This vulnerability has many facets and this article presents only an overview. More details are available in the external links at the end.

Be aware that:

- It is technically an attack against a single browser, not the server. The most likely goal of an attack is to retrieve an encrypted session cookie in order to hijack a user's session.
- While a "practical" attack has been demonstrated, it is not a simple attack. It involves man-in-the-middle network access in conjunction with a certain amount of control over the user's browser to have it make repeated requests with content under the attacker's control, as well as heavy real-time computing power. The attack vector was known previously but not considered usable.
- The attack applies only to CBC (cipher block chaining) algorithms as implemented in SSL 3.0 and TLS 1.0. The streaming cipher RC4 is not vulnerable, and newer versions of TLS implement CBC in ways that are resistant to this attack. However, some cryptographers consider RC4 weaker than the CBC algorithms (AES and DES), while implementation of TLS 1.1+ is uncommon.
- Browser (and component) makers are taking steps to close the vectors that allow attackers the kind of access needed and implement TLS 1.1+.

Resolution

As this is a browser-side attack, you have these options to mitigate the possibility of an attack:

- **Require TLS 1.1+**
  If available, you can specify that only TLS 1.1+ ciphers be used by your server with the *SSLCipherSuite* directive (more about directives in the next section). It is not good enough to just enable TLS 1.1+ as an option alongside TLS 1.0/SSL 3.0, as it is fairly easy for a MITM to force a protocol downgrade to an available vulnerable protocol.

  Note: Most browsers do not implement these protocols and would be unable to access sites requiring the newer protocols. This is only an option where you either control the browsers/clients or do not care if the site is unavailable to incompatible browsers. It is also only an option with OpenSSL 1.0.1 and greater (which is beta and not included in any VMware releases at time of writing).

- **Use the RC4 cipher**
  You can specify which ciphers your server will allow or prefer. The RC4 cipher is a stream cipher and is not vulnerable to this attack. However, there has been some debate about its strength and security. It is up to you to determine whether it suits your needs.

  To allow only RC4 ciphers for your SSL server, you can specify the allowed ciphers with the *SSLCipherSuite* directive in your SSL configuration:

  ```
  SSLCipherSuite !aNULL:!ADH:!eNULL:!LOW:!EXP:!SSLv2:RC4+RSA
  ```

  This allows only a very limited set of ciphers. RC4 is widely implemented, but if some users have disabled it, they are unable to access your site. A less restrictive strategy might be to prefer RC4 but allow others. To do this, add the *SSLHonorCipherOrder* directive (which ignores the browser's preference of cipher in favor of the server ordering):

  ```
  SSLCipherSuite !aNULL:!ADH:!eNULL:!LOW:!EXP:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:ALL
  ```
  SSLHonorCipherOrder on SSL connections use RC4 unless the browser does not support it, in which case the handshake falls back to other strong ciphers.

- **Reduce the lifespan of the SSL session**

  The BEAST attack involves repeated requests on the same SSL session to progressively decrypt plaintext over a span of minutes. This attack is disrupted by lowering the session life, forcing a new SSL handshake more often. Reducing the session life may mean a decrease in performance, but lowering the default *SSLSessionCacheTimeout* (5 minutes) to 30 seconds, or even lower, should not be too severe. However, it is up to you to determine the impact for your specific situation.

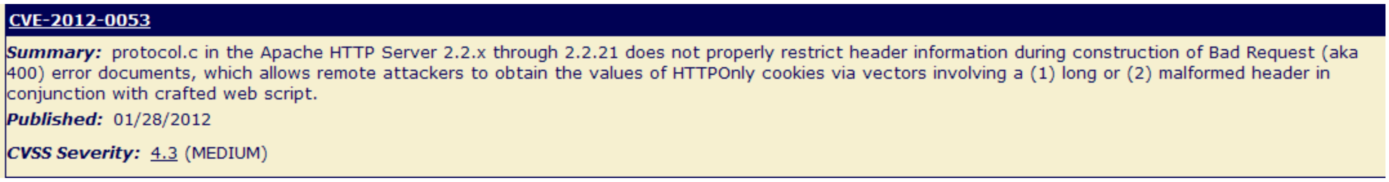
CVE-2012-0053 (Apache HTTP Server httpOnly information disclosure)

- **Refer to:** http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0053
  http://www.securityfocus.com/bid/51706
- Applies to Apache versions 2.2.x through 2.2.21 (Fixed in Apache 2.2.22)
- “Upgrade to Apache HTTP Server version 2.2.22 or newer.”

Products

- **1200 SecureSyncs and 9400s:**
  - Apache was updated to version 2.2.23 in SecureSync software update version 4.8.8 to fix this issue. Versions 4.8.8 and above are not susceptible.

- **9300/9200:** Apache was updated to v2.2.22 with the version 3.6.0 update. Not applicable to software versions 3.6.0 and above.



CVE-2012-0053

Summary: protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.

Published: 01/28/2012

CVSS Severity: 4.3 (MEDIUM)

Email from Bill Glase to Dick Fox (10/16/12)
CVE-2012-0053 refers to a vulnerability identified earlier this year in the Apache web server (versions 2.2.x through 2.2.21). Details are available online (http://www.cvedetails.com/cve/CVE-2012-0053/). Depending upon the specific Apache configuration, and the design of the web application, the vulnerability may allow unauthorized access to a specific class of cookie (user data) known as an httpOnly cookie.

The presence of the vulnerability on the report means that the scanner identified the version of Apache as matching one of those above, not that the vulnerability actually exists in the device being scanned, or that it can be exploited. The vulnerability cannot be exploited in the Spectracom device because:

- The Spectracom device does not use httpOnly cookies. If a server (the Spectracom device) uses this type of cookie, it signals to the user's browser that it should restrict access to the information in the cookie (mainly from being accessed via javascript). Because the Spectracom device does not require this restriction, there is no loss of security as a result of the Apache bug.

- Exploiting the vulnerability requires XSS (cross-site scripting) techniques. Because the Spectracom device does not allow unauthorized requests (users must be logged in before any request can be made), and does not allow users to store 'active' content that could contain malicious scripting, it is not possible to trigger the security vulnerability above.

Our normal security updates will address this issue so that it will not appear on vulnerability scans in the future. The update should be available near the end of this calendar year.

Keith's earlier response (10/16/12): The current Apache version is version 2.2.21, with this potential vulnerability mitigated in version 2.2.22. We are discussing updating Apache to a more recent version with the next NetClock software upgrade. At this time, the next NetClock software version upgrade is tentatively scheduled for the December 2012 time-frame.

I have created Salesforce case number 00006434 (and flagged it to remind us to let you know that your customer will need the next software update to mitigate this potential vulnerability).

Note that we have been recently looking into this one (one other customer recently reported this, as well). This appears to be a very low risk vulnerability, as it is not a means to gain access to the NetClock. It is associated with a header of a generic error message being displayed. The other customer understands the low risk and is not preventing them from connecting it to their network. If your customer is concerned with this low risk vulnerability, I suspect it will mitigated with the December time-frame software update.

Refer to: Dany Loke with Roots (Case 6327) and Maoun Charbel (case 6434).

Summary: protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.
Fix: upgrade Apache to version 2.2.22
Risk: Moderate (4.3 out of 10)

Products:

- **SecureSyncs:**

SecureSyncs with at least software versions 4.8.7 and below installed.

Note (10/8/12 KW)**:** SecureSync upgrade to Apache v2.2.22 (or a possible patch to fix in current Apache v2.2.21) unknown/unplanned as of this moment.

- **NetClocks (9300 and 9200 series):**

  NetClocks with software versions 3.5.0 and below installed.

  Note: (10/8/12 KW) soon to be released NetClock software upgrade (v3.5.1) is updating Apache to v2.2.22 which will mitigate this CVE.

“Certificate cannot be trusted” and “SSL Self-signed certificate”

Refer to the HTTPS document for NetClock and SecureSync:

This report just indicates you haven’t purchased a SSL certificate from a company such as **VeriSign.com** or **godaddy.com**, (as two examples). Instead, you followed the directions that we sent to you to allow you to create your own “self-signed” SSL certificate. However, you can also have the abilty purchase a certificate to clear this report,

If desired, you can create a SSL certificate request that can be exported and sent to another company that allows you to purchase a SSL certificate. They will send you the certificate to install.

Both of these two items can be resolved by purchasing an SSL certificate, instead of using the one you have created.

Prevent Cross Site Request Forgery (CSRF) attacks

(cross-site)

Severity

A) SecureSyncs/9400s

- Refer to JIRA case SSS-599
- addressed in version 5.8.5 update

CVE-2012-1823 (PHP 'php-cgi' Information Disclosure Vulnerability)

- Refer to Salesforce case 12717 (https://na8.salesforce.com/500C000000VNTs7)
- Reported Dec, 2013

We have one of your NetClock appliances. I have been tasked with finding what OS runs on our "appliance" type devices and also to see if the device could be affected by the **Linux Worm Darlloz.**

Listed below are some articles that explain the findings:

http://www.symantec.com/security_response/writeup.jsp?docid=2013-112710-1612-99&tabid=2

http://www.cio.com/article/743858/Worm_Targets_Linux_PCs_and_Embedded_Devices?taxonomyId=3089

http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices

http://www.computerworld.com/s/article/9244503/Worm_may_create_an_Internet_of_Harmful_Things_says_Symantec_Take_note_Amazon_

http://www.scmagazine.com/linux-worm-discovered-capable-of-infecting-internet-enabled-home-devices/article/323404/

http://arstechnica.com/security/2013/11/new-linux-worm-targets-routers-cameras-internet-of-things-devices/

http://www.dd-wrt.com/wiki/index.php/Supported_Devices

http://www.securityfocus.com/bid/53388

http://www.cyberdefensemagazine.com/internet-of-things-symantec-has-discovered-a-new-linux-worm/#sthash.x11t62wl.dpbs

http://www.itproportal.com/2013/12/04/linux-malware-found-that-can-infect-home-appliances/

http://www.itwire.com/opinion-and-analysis/the-linux-distillery/62481-symantec-identifies-internet-of-things-worm

http://www.securityweek.com/linux-worm-targets-internet-things

Email from Paul Myers (16 Dec 2013) Executive Summary:
Executive Summary:

Linux (Gentoo) releases 5.x.x uses PHP package version 5.3.23.
Our Version 5.3.23 is not impacted on new SecureSync version. (see below)
NetClock 93xx units do NOT use PHP and are not impacted.
SecureSync 4.x.x used PHP 5.3.8 if built on Brutal Linux build 2.7.0 or later from June 2012

However, I think ONLY the update page used PHP?

I don’t think we would be impacted if:

HTTPS is used and HTTP is disabled
ONLY the update page that I know of during updates might be at risk?
Confirm with David Sohn?

Defect Details:

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1823
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1823

sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.

https://bugs.php.net/bug.php?id=61910

PHP reports it is fixed in 5.4.3

CVE-2012-4929 / CVE-2012-4930 TLS CRIME Vulnerabilities (TLS version 1.2)

- Refer to Mantis case 1898: http://cvsmantis.int.orolia.com/mantis/view.php?id=1898
- (8 Apr 2013 KW) As of Archive version 4.8.9, these two vulnerabilities have not yet been mitigated.

- Refer to: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4929

Description: The TLS protocol 1.2 and earlier, as used in Mozilla Firefox, Google Chrome, Qt, and other products, can encrypt compressed data without properly obfuscating the length of the unencrypted data, which allows man-in-the-middle attackers to obtain plaintext HTTP headers by observing length differences during a series of guesses in which a string in an HTTP request potentially matches an unknown string in an HTTP header, aka a "CRIME" attack.

Severity

CVE-2012-4930

Refer to http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4930

Description:The SPDY protocol 3 and earlier, as used in Mozilla Firefox, Google Chrome, and other products, can perform TLS encryption of compressed data without properly obfuscating the length of the unencrypted data, which allows man-in-the-middle attackers to obtain plaintext HTTP headers by observing length differences during a series of guesses in which a string in an HTTP request potentially matches an unknown string in an HTTP header, aka a "CRIME" attack.

Email from Lisa Perdue to Danny Loke (22 Apr 13)
I have found this information on the vulnerabilities:

All major web browsers have either been patched or do not support SSL/TLS compression at all. Because of this, the industry standard is to disable compression at the client level.

Ensure that administrators who will actively connect to a host's web page use these browser versions or higher:

Internet Explorer: No versions of IE support SSL/TLS Compression
Chrome: 21.0.1180.89
Firefox: 15.0.1
Opera: 12.01
Safari: 5.1.7

In summary- So it appears that the issue can be corrected on the client side by updating to a newer web browser. I know that that customer still needs the SecureSync updated in order to pass the security scan tested but I hope they can be comforted that they are not actually vulnerable if they use an updated browser. We are working on building a new release with updated Apache. The Case 00009073 is still flagged to notify you and the customer when the release becomes available.

CVE-2013-0169

(12 Mar 2013 KW, reported by Muhammad Sallam)

- **Refer to:** Mantis Case **1966** for SecureSync and NetClock 9400s http://cvsmantis.int.orolia.com/mantis/view.php?id=1966
- **Refer to:** Fogbugz Case **1851** for NetClock 9300s
- **Refer to:** http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0169

Severity

Affected OpenSSL versions: OpenSSL prior to version 1.0.1d (1.01d and above mitigates)
The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding.
Products:

- ○ **SecureSyncs: Version 4.8.8 uses SSL version 1.0.1c, so it's affected. Fix is in software versions of at least version 5.0.0- which updated OpenSSL to v1.0.1e (may have been fixed prior to 5.0.0 but I don't have any notes on OpenSSL in versions before 5.0.0).**
- ○ **NetClocks (9300 and 9200 series): The version 3.6.1 update upgraded SSL to version1.0.1C. This version is susceptible to this potential vulnerability. A post v3.6.1 upgrade will need to update SSL to a newer version, if we decide to release another version of software.**

CVE-2013-2566 (SSL/TLS use of weak RC4 cipher)

(2 May 2013, reported by Gary Brinkley)

Note: "RC4" is also referred to as "ARC4"

NOTE: there are at least a few different CVEs associated with the RC4 (ARC4) cipher

- ➢ FOR MORE INFO ON RC4/ARC4, REFER TO (in this doc) **RC4 (also known as ARC4 or ARCFour)
- ➢ In summary of this link, the software should be at version 5.2.0 or higher and the classic web browser interface needs to be "DISABLED" in Services.
- ➢ for more info on this particular CVE, refer to Mantis case: 1996 http://cvsmantis.int.orolia.com/mantis/view.php?id=1996
- ➢ Refer to: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2566 or http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2566

Description: The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g. HTTP cookies), and an attacker is able to obtain many (i.e. tens of millions) ciphertexts,
the attacker may be able to derive the plaintext.

Severity

Products:

- ○ **1232 VelaSyncs/VersaSyncs: ??**
- ○ **SecureSyncs: REFER ALSO TO (in this doc) **RC4 (also known as ARC4 or ARCFour)**

Details

- RC4 (ARC4) algorithm was initially removed in 1200 SecureSync/9400 version 5.0.1 (and above). Refer to Mantis case 2293)
- RC4 was then inadvertently brought back into the software with **version 5.1.5** (Refer to Mantis case 2918). It is also confirmed to be enabled in **versions 5.1.7 and 5.1j** as well.
- Applicable to 1200 SecureSync/9400 with RC4 cipher enabled. These are ones with:
- Software Versions 5.15, 5.1.6, 5.1.7 and 5.1J which have RC4 installed.
- Software **Versions 5.0.0 and below** have RC4 installed.

Email from Keith to Ron, Dave s and Oleg, **(16 Jan 2015)** RC4 (ARC4) was removed in version 5.0.1 as a weak cipher (Mantis 2293) It was then inadvertently added back in with the version 5.1.5 update (Mantis 2918). I just checked 5.1J and it has it enabled, also.

Follow-up Email from Keith (19 Jan 2015) Thanks for your email regarding CVE-2013-2566. For your information, **we expect this potential vulnerability to be resolved in the next (version 5.2.0)** SecureSync software update, which is still planned to be available around the end of January. We will let you know when the version 5.2.0 software update has been made available.

- **NetClocks (9300 and 9200 series): ??**
- **legacy VelaSyncs: ?**

CVE 2014-0195 (dtls1_reassemble_fragment function)

- Refer to Mantis case 2854 http://cvsmantis.int.orolia.com/mantis/view.php?id=2854
- Refer to sites such as: http://www.rapid7.com/db/modules/auxiliary/scanner/ssl/openssl_ccs or https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=687

Severity

Affected OpenSSLVersion(s): OpenSSL prior to version 1.0.1i (1.01i and above mitigates)

From the second link above:

- OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za.
- OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m.
- OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h.

Products:

- **SecureSync/948x**

  versions 5.1.5 and below (v5.1.5 has OpenSSH v1.0.1h). Fix is in version 5.1.6 and above (v5.1.6/5.1.7 upgrades update OpenSSL to version 1.0.1i which mitigates this CVE)

- **9300 series:**

  NetClocks with versions 3.6.6 and below installed (fix is in version 3.6.7 and above. V3.6.7 updated OpenSSL to v1.01j)

CVE 2014-0198 (do_ssl3_write function in s3_pkt.c)

- AKA "CWE-119"
- Refer to Salesforce case 16758.
- Refer to Mantis case 2854 http://cvsmantis.int.orolia.com/mantis/view.php?id=2854
- Refer to sites such as: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0198

Severity

Affected OpenSSLVersion(s): OpenSSL 1.x through 1.0.1g (1.01h and above mitigates)

Products:

- **SecureSync/948x**
  - **Versions 5.1.5 and below (v5.1.5 has OpenSSH v1.0.1h). Fix is in version 5.1.6 and above (v5.1.6/5.1.7 upgrades update OpenSSL to version 1.0.1i which mitigates this CVE)**
- **9300 series:**
  - **NetClocks with versions 3.6.6 and below installed (fix is in version 3.6.7 and above. V3.6.7 updated OpenSSL to v1.01j)**

CVE 2014-0221 (do_ssl3_write function in s3_pkt.c)

- Refer to: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0221

Overview: The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.

Affected OpenSSLVersion(s):

```
 OpenSSL 0.9.8 DTLS users should upgrade to 0.9.8za
 OpenSSL 1.0.0 DTLS users should upgrade to 1.0.0m.
 OpenSSL 1.0.1 DTLS users should upgrade to 1.0.1h.
```

Severity

Products:

- **SecureSync/948x**
- **9300 series:**

  NetClocks with versions 3.6.6 and below installed are affected (fix is in version 3.6.7 and above. V3.6.7 updated OpenSSL to v1.01j)

CVE-2014-0224: 'ChangeCipherSpec' MiTM Vulnerability/OpenSSL Server-Side ChangeCipherSpec Injection Scanner

- Refer to Salesforce case 16758.
- Refer to Mantis case 2854 http://cvsmantis.int.orolia.com/mantis/view.php?id=2854
- Refer to sites such as: http://www.rapid7.com/db/modules/auxiliary/scanner/ssl/openssl_ccs
- https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=687

Affected OpenSSLVersion(s): OpenSSL prior to version 1.0.1i (1.01i and above mitigates)

From the second link above:

- OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za.
- OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m.
- OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h.

Severity

Products:

- **SecureSync/948x**

  Versions 5.1.5 and below (v5.1.5 has OpenSSH v1.0.1h). Fix is in version 5.1.6 and above (v5.1.6/5.1.7 upgrades update OpenSSL to version 1.0.1i which mitigates this CVE)

- **9300 series:**

  NetClocks with versions 3.6.6 and below installed (fix is in version 3.6.7 and above. V3.6.7 updated OpenSSL to v1.01j)

CVE 2014-3470 (do_ssl3_write function in s3_pkt.c)

- Refer to Salesforce case 16758.
- Refer to Mantis case 2854 http://cvsmantis.int.orolia.com/mantis/view.php?id=2854
- Refer to sites such as: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3470
- https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=687
- Affected OpenSSLVersion(s): OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h

Severity

Affected OpenSSLVersion(s): OpenSSL prior to version 1.0.1i (1.01i and above mitigates)
From the second link above:

- OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za.
- OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m.
- OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h.

Products:

- **SecureSync/948x Versions 5.1.5 and below (v5.1.5 has OpenSSH v1.0.1h). Fix is in version 5.1.6 and above (v5.1.6/5.1.7 upgrades update OpenSSL to version 1.0.1i which mitigates this CVE)**

- **9300 series NetClocks with versions 3.6.6 and below installed (fix is in version 3.6.7 and above. V3.6.7 updated OpenSSL to v1.01j)**

CVE-2014-3505, CVE-2014-3506, CVE-2014-3507, CVE-2014-3508, CVE-2014-3509, CVE-2014-3510, CVE-2014-3511, CVE-2014-3512, CVE-2014-5139

- Refer to Mantis case 2891 http://cvsmantis.int.orolia.com/mantis/view.php?id=2891

Severity

Affected OpenSSLVersion(s): OpenSSL prior to version 1.0.1i (or higher with some) (1.01i and above mitigates)

Products:

- **SecureSync/948x**

  Versions 5.1.5 and below (fix is in version 5.1.6 and above. 5.1.6 updated OpenSSL to v1.0.1i)

- **9300 series**

  NetClocks with versions 3.6.6 and below installed (fix is in version 3.6.7 and above. V3.6.7 updated OpenSSL to v1.01j)

CVE-2014-3566 (Poodle)

- Refer to Mantis case 2927 http://cvsmantis.int.orolia.com/mantis/view.php?id=2927

Severity

Affected OpenSSLVersion(s): OpenSSL versions 1.0.1i and below

Products:

- **SecureSync/948x**

  Versions 5.1.7 and below are susceptible. Versions 5.2.0 and above are not susceptible (update version 5.2.0, Feb 2015, upgraded OpenSSL to version 1.0.1k which mitigates Poodle.)

  Notice: The **classic interface** web browser should be disabled (via the slider on the left-side of the Management -> Network setup page of the browser). If this potential vulnerability is detected with software verisons 5.2.0 and above installed, the classic interface vrowser must have since been enabled by a user

- **9300 series:**

  NetClocks with at least versions 3.6.6 and below installed. Fix is in version 3.6.7 and above. (V3.6.7 updated OpenSSL to v1.01j).

CVE-2014-3569 (Null pointer Derefence)

- Refer to Mantis case 2959: http://cvsmantis.int.orolia.com/mantis/view.php?id=2959
- **Refer to:** http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3569
- AKA “CWE-476” (http://cwe.mitre.org/data/definitions/476.html

Severity

Affected OpenSSLVersion(s): OpenSSL 0.9.8zc, 1.0.0o, and 1.0.1j (mitigated in 1.0.1k)

Products:

- **SecureSync/948x**

  Versions 5.1.7 and below are susceptible (update version 5.2.0, Feb 2015, upgraded OpenSSL to version 1.0.1k which mitigates it.)

- **9300 series:**

  NetClocks with at least versions 3.6.7 and below installed.

CVE-2014-3570 (BN_sqr implementation)

- Refer to Mantis case 2959: http://cvsmantis.int.orolia.com/mantis/view.php?id=2959
- **Refer to:** http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3570

Severity

Affected OpenSSLVersion(s): OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k (mitigated in 1.0.1k)

Products:

- **SecureSync/948x**

  Versions 5.1.7 and below are susceptible (update version 5.2.0, Feb 2015, upgraded OpenSSL to version 1.0.1k which mitigates it.)

- **9300 series:**

  NetClocks with at least versions 3.6.7 and below installed.

CVE-2014-3571 (Null pointer Derefence)

- Refer to Mantis case 2959: http://cvsmantis.int.orolia.com/mantis/view.php?id=2959
- **Refer to:** http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3571

Severity

Affected OpenSSLVersion(s): OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k (mitigated in 1.0.1k)

Products:

- **SecureSync/948x**

  Versions 5.1.7 and below are susceptible (update version 5.2.0, Feb 2015, upgraded OpenSSL to version 1.0.1k which mitigates it.)

- **9300 series:**

  NetClocks with at least versions 3.6.7 and below installed.

CVE-2014-3572 (ssl3_get_key_exchange)

- Refer to Mantis case 2959: http://cvsmantis.int.orolia.com/mantis/view.php?id=2959
- **Refer to:** http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3572

Summary:

Severity

- **Affected OpenSSLVersion(s):** OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k (mitigated in 1.0.1k)

Products:

- **SecureSync/948x**

  Versions 5.1.7 and below are susceptible (update version 5.2.0, Feb 2015, upgraded OpenSSL to version 1.0.1k which mitigates it.)

- **9300 series:**

  NetClocks with at least versions 3.6.7 and below installed.

CVE-2014-8176 (dtls1_clear_queues function)

- Refer to https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-8176 and https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8176

Summary: The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.

Severity:

Affected OpenSSLVersion(s): OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h (mitigated in 1.0.1h)

Products:

- **SecureSync/948x**

  Versions 5.1.7 and below are susceptible (update version 5.1.5 upgraded OpenSSL to version 1.0.1h which mitigates it. But version 5.1.5 wasn't released to manufacturing. The next more recent version to be cut-in was 5.1.7)

- **9300 series:**

  Versions 3.6.6 and below are susceptible (version 3.6.7, Oct 2014, upgraded openssl to version 1.0.1j)

CVE-2014-8275

- Refer to Mantis case 2959: http://cvsmantis.int.orolia.com/mantis/view.php?id=2959
- **Refer to:** http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-8275

Affected OpenSSLVersion(s): OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k (mitigated in 1.0.1k)

Severity:

Products:

- **SecureSync/948x**

  Versions 5.1.7 and below are susceptible (update version 5.2.0, Feb 2015, upgraded OpenSSL to version 1.0.1k which mitigates it.)

- **9300 series:**

  NetClocks with at least versions 3.6.7 and below installed.

-- ----------

CVE-2014-8730 (a variant of Poodle)

- **Refer to:** http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-8730

Per Oleg (15 Dec 2014) The vulnerability requires a man-in-the-middle attack against TLS 1.x connections that use CBC ciphers and could allow the attacker to calculate some of the plaintext communication. We do not allow CBC ciphers, so we **ARE NOT** vulnerable.

Severity:

Products:

- ○ SecureSyncs and 9400s:
  SecureSyncs with at least software versions 5.1.4 and below installed.

- ○ **NetClocks (9300 and 9200 series)**

  NetClocks with at least software versions 3.6.7 and below installed.

-- ----------

ICS-CERT Advisory (ICSA-14-353-01) CVE-2014-9296, CVE-2014-9295 CVE-2014-9294, CVE-2014-9293

- Dec, 2014
- Link to advisory: https://ics-cert.us-cert.gov/advisories/ICSA-14-353-01

Severity:

Products:

- ○ **SecureSyncs and 9400s:**

  SecureSyncs with at least software versions 5.1.4 and below installed.

- ○ **NetClocks (9300 and 9200 series):**

  NetClocks with at least software versions 3.6.7 and below installed.

-- ----------

CVE-2015-0204 and CVE-2015-1067 ("Freak attack") (ssl3_get_key_exchange function)

- **Refer to** Mantis case 2959: http://cvsmantis.int.orolia.com/mantis/view.php?id=2959
- **Refer to:** http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0204
- **Affected OpenSSLVersion(s):** OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k (mitigated in 1.0.1k)

Severity:

Products:

- ○ **SecureSync/948x**

Versions 5.1.7 and below are susceptible (update version 5.2.0, Feb 2015, upgraded OpenSSL to version 1.0.1k which mitigates it).

Notice: The **classic interface** web browser should be disabled (via the slider on the left-side of the Management -> Network setup page of the browser). If this potential vulnerability is detected with software verisonss 5.2.0 and above installed, the classic interface vrowser must have since been enabled by a user.

- **9300 series:**

  NetClocks with at least versions 3.6.7 and below installed.

  Per Dave Sohn, 9 March 2015 (regarding SecureSync 5.2.0 and NetClock version 3.6.7): Looking at scanning tools checking specifically for the FREAK attack, the current versions of 1200 SecureSync/9400 and 9200/9300 are not vulnerable.

  https://www.ssllabs.com/ssltest/analyze.html?d=time2.spectracomcorp.com
  https://www.ssllabs.com/ssltest/analyze.html?d=time.spectracomcorp.com
  https://tools.keycdn.com/freak

CVE-2015-0205 (ssl3_get_cert_verify function) Man in the Middle Security Bypass Vulnerability

- **Refer to** Mantis case 2959: http://cvsmantis.int.orolia.com/mantis/view.php?id=2959
- **Refer to:** http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0205
- **Affected OpenSSLVersion(s):** OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k (mitigated in 1.0.1k)

Severity:

Products:

- **SecureSync/948x**

  Versions 5.1.7 and below are susceptible (update version 5.2.0, Feb 2015, upgraded OpenSSL to version 1.0.1k which mitigates it.)

- **9300 series:**

  NetClocks with at least versions 3.6.7 and below installed.

CVE-2015-0206 (Memory leak in the dtls1_buffer_record function)

- Refer to Mantis case 2959: http://cvsmantis.int.orolia.com/mantis/view.php?id=2959
- Refer to: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0206

Affected OpenSSLVersion(s): OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k (mitigated in 1.0.1k)

Severity:

Products:

- **SecureSync/948x**

Versions 5.1.7 and below are susceptible (update version 5.2.0, Feb 2015, upgraded OpenSSL to version 1.0.1k which mitigates it.)

- **9300 series:**

  NetClocks with at least versions 3.6.7 and below installed.

CVE-2015-0235 (AKA “Ghost”) glibc gethostbyname buffer overflow

Heap-based buffer overflow in the __nss_hostname_digits_dots function in glibc 2.2, and other 2.x versions before 2.18, allows context-dependent attackers to execute arbitrary code via vectors related to the (1) gethostbyname or (2) gethostbyname2 function, aka "GHOST."   detected in the GNU / Linux C Library (glibc)

- Refer to the following links for details:

  http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0235
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0235
  http://ma.ttias.be/critical-glibc-update-cve-2015-0235-gethostbyname-calls/
  http://www.openwall.com/lists/oss-security/2015/01/27/9

Severity:

Products:

Note (applicable to SecureSyncs, 9400s. 9300 and 9200s): scanning/testing shows that with versions 5.1.7 and 3.6.7, the only test for Ghost that is failing is the report that the version of the glibc is vulnerable. But all other tests for Ghost are showing no other vulnerabilities. So software versions 5.1.7 and below and 3.6.7 and below are not vulnerable

- **Legacy VelaSync**

  (from Version 7.0.0 Release Notes): Basepackage upgrade (version 1.3) for TimeKeeper Grandmasters available to address GHOST glibc vulnerability (CVE-2015-0235)

- **SecureSync/948x**

  Versions 5.1.7 and below (fix for the file version is in 5.2.0 and above. ~9 Feb, 2015). Glibc was updated from 2.15 to 2.19 in upgrade version 5.2.0.

- **9300 series:**

  NetClocks with at least versions 3.6.7 and below installed (all versions as of Jan , 2015)   Engineering is investigating

----

CVE-2015-1637 (also associated with “Freak Attack)

- Refer to: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1637
- Related to CVE-2015-0204 and 2015-1067 (“freak attack”) but a different vulnerability.
- This CVE does not apply to us. This one is specific to only certain versions of **Windows**

CVE-2015-2808 (BAR Mitzvah attack associated with the RC4 cipher)

- Refer to: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2808 and http://www.secpod.com/blog/cve-2015-2808-bar-mitzvah-attack-in-rc4-2/

The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue.

Severity:

Products:

○ **SecureSync/948x**

In summary- the fix for this CVE requires BOTH of the following items:

1. **Software be updated to version 5.2.1 or higher (to have the switch available that can disable the classic UI)**
2. **Classic interface web browser be disabled via a switch in the newer browser (in the bottom-left side Management -> Network page)**

Detail:

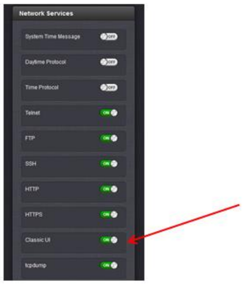
Versions 5.2.0 and below are susceptible, as well as versions 5.2.1 and above if the Classic Interface web browser hasn't been disabled in the newer web browser.

Fix is to update the software to at least version 5.2.1 and to also disable the Classic Interface browser. Refer to "RC4" further below in this document for additional info on RC4 cipher and disabling the classic interface browser. RC4 is not present in versions 5.2.1 and above once the Classic Interface browser has been disabled.

How to disable classic interface browser:

Email from Keith to a customer (10 Mar 16) CVE-2015-2808 was addressed in the version 5.2.1 software update, when the classic interface browser has been disabled (this version of software added the ability to disable the classic interface browser access via a button in the newer black background web browser).

With software version 5.2.1 or above installed, to disable access to the classic interface browser, in the newer browser navigate to the **Management** -> **Network** page. In the bottom-left corner, change the slider switch for "**Classic UI**" to the OFF position. Port "8080" is now closed, so the classic interface browser is no longer accessible.



Network Services

System Time Message OFF

Daytime Protocol OFF

Time Protocol OFF

Telnet ON

FTP ON

SSH ON

HTTP ON

HTTPS ON

Classic UI ON

tcpdump ON

○ **9300 series: ??**

CVE-2015-4000 TLS Diffie-Hellman Key Exchange Logjam Vulnerability (RC4 cipher)

- This CVE is associated with the "**RC4"** cipher
- RC4 was removed in SecureSync update version 5.2.1 for the newer browser. But is still available for the classic interface browser, so the Classic interface browser needs to be disabled in the newer browser to remove this cipher from being available (at least until a future software update has removed the classic interface),
- Refer to "RC4" (in the "**Security Algorithms**" Section) in the SecureSynccustassist doc for details on this CVE and on how to disable the Classic interface browser

Severity:

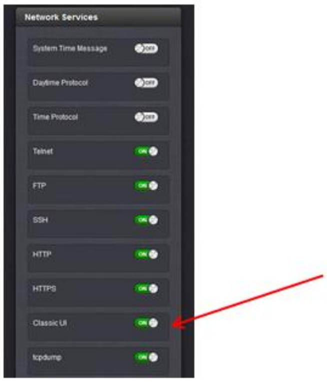
Products:

- **SecureSync/948x**

  In summary: the fix for this CVE requires BOTH of the following items:

  1. **Software be updated to version 5.2.1 or higher**
  2. **Classic interface web browser be disabled via a switch in the newer browser**

     How to disable classic interface browser:
     Email Keith sent to a customer (10 Mar 16) To disable complete access to the classic interface browser, in the newer browser navigate to the **Management** -> **Network** page. In the bottom-left corner, change the slider switch for "**Classic UI**" to the OFF position. Port "8080" is now closed, so the classic interface browser is no longer accessible.



Network Services

System Time Message OFF
Daytime Protocol OFF
Time Protocol OFF
Telnet ON
FTP ON
SSH ON
HTTP ON
HTTPS ON
Classic UI ON
tcpdump ON

With the classic interface browser now disabled, all browser access will be via the newer black background web browser. Rescan and you should see this potential vulnerability is no longer present.

Note that in order to use the newer web browser with Internet Explorer, IE may need to be updated to a much more recent version (we recommend IE 10 or higher) to be fully compatible with the newer browser.

- **9300 series: ???**

CVE-2015-9251 (jQuery vulnerability)

- ➢ Refer to sites such as https://nvd.nist.gov/vuln/detail/cve-2015-9251

Description jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed

Severity:

Products:

- ○ **2400 SecureSyncs**
- ○ **Legacy VelaSyncs**
- ○ **1200 SecureSyncs and 9400s**
- ○ **At least versions 5.9.5 and below appear affected**
  - ○ Refer to Salesforce Cases such as
  - ○ Refer to JIRA **SSS-1178** (looking at fix in 5.9.6 towards Middle of 2023)

- ○ **NetClock 9300 and 9200 series**

--- ---------

CVE-2006-20001 (Apache)

- Refer to sites such as https://nvd.nist.gov/vuln/detail/CVE-2006-20001
- Refer to Salesforce Case 292984

Severity: High

Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash. This issue affects Apache HTTP Server 2.4.54 and earlier.

Known affected Apache server software versions: Apache HTTP Server 2.4.54 and earlier.

Products:

- **2400 SecureSyncs/VersaSync**
  - **Refer to CAR-2238 (Feb 2023)**

    CAR-2238 closed. Note from Ryan Johnson added to ticket when it was closed: "*None of these modules are used in SS2400/Versa and therefore do not impact us"*

- **1200 SecureSync/9400s**
  - **Refer to SSS-1320 (Feb 2023)**

    SSS-1320 closed. Note from Ryan Johnson added to ticket when it was closed: "*None of these modules are used in SS1200 and therefore do not impact us*"

S/S Version	Apache version
5.9.6	
5.9.5	Updated to **2.4.53**
5.9.3/5.9.4	Updated to **2.4.48**
5.9.0	Updated to **2.4.41**
5.8.1	Updated to **2.2.31**

- **1232 VelaSyncs:**

- **NetClock 9300 and 9200 series**: