# Security of Timing Infrastructure – Network based threats and CVEs

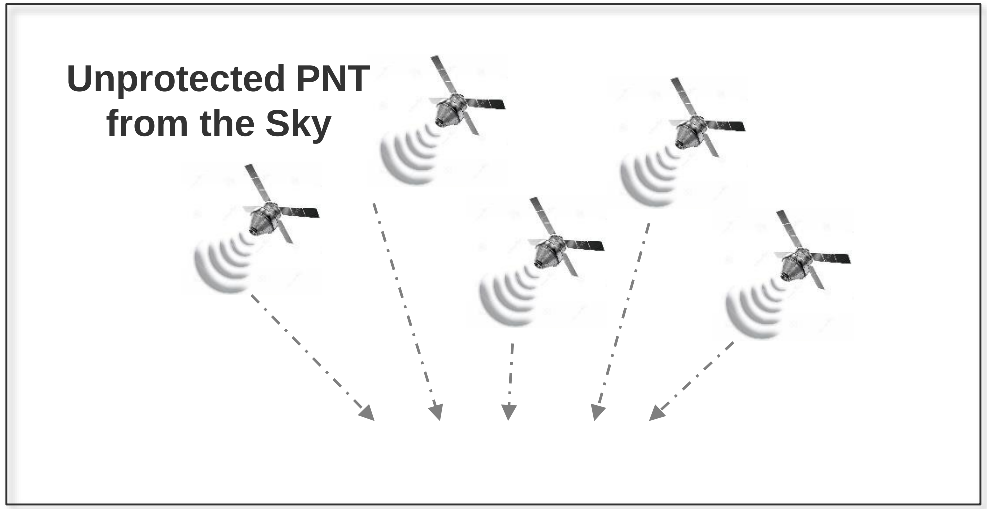
**Barry Dropping**

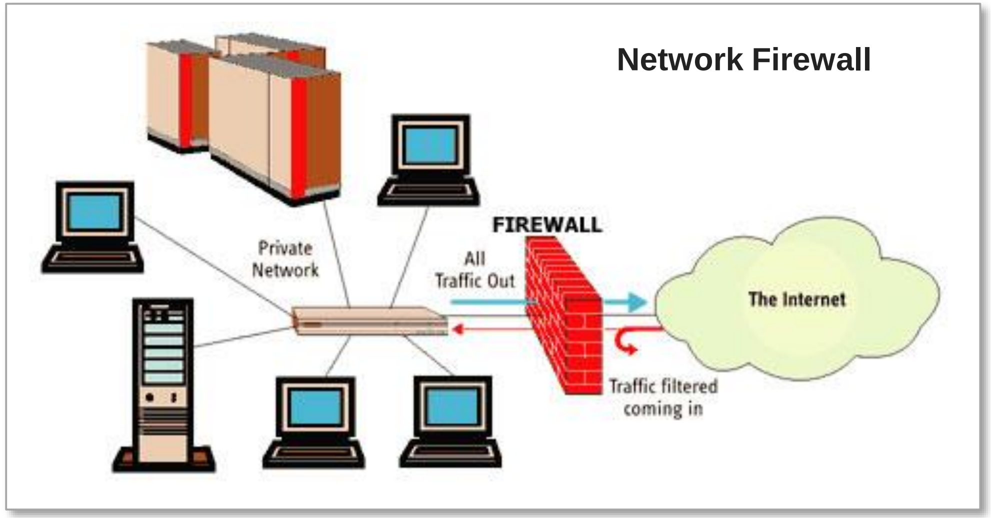
**March 2019**

# Agenda

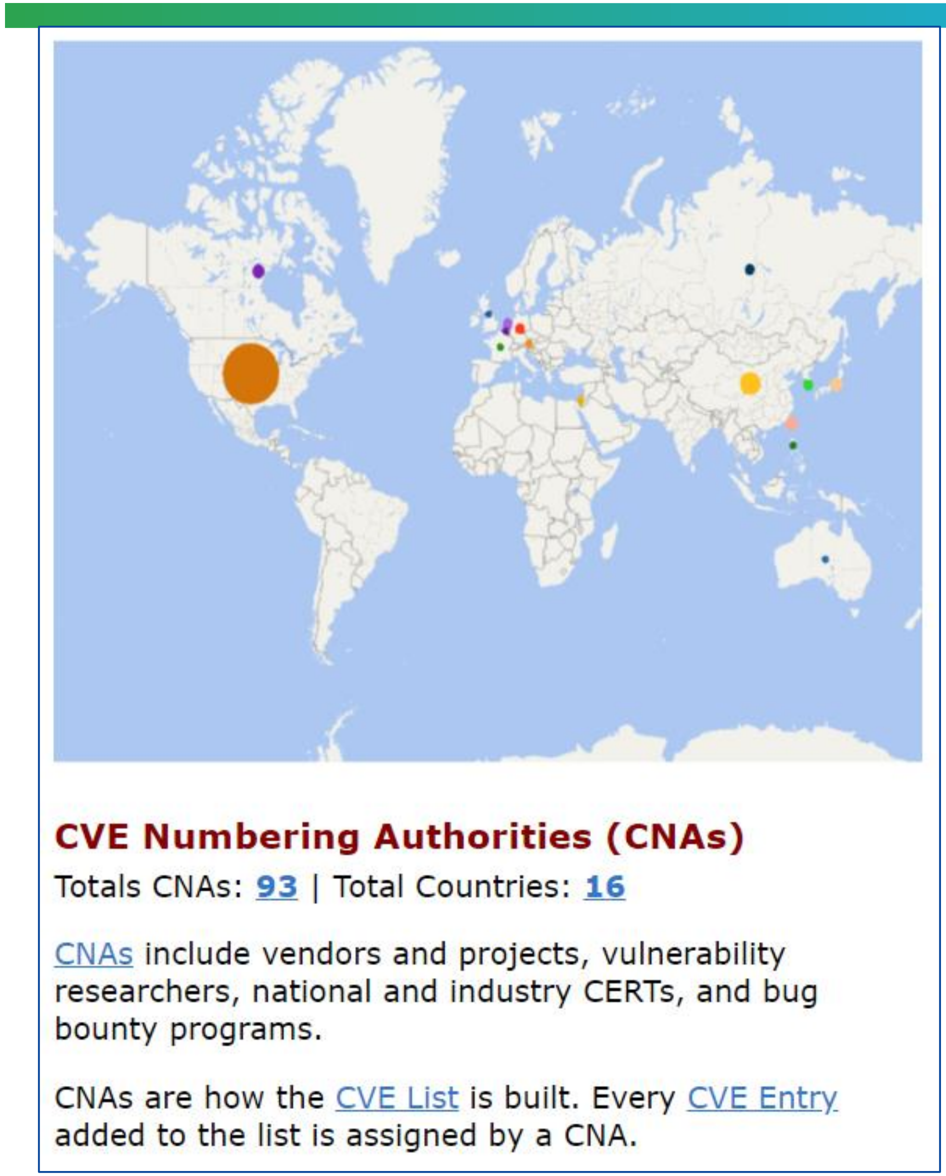
- “Security Perimeter” of network based time servers
- Common Vulnerabilities and Exposures (CVE) Update
- Best practices in addressing CVEs
- Additional security requirement in the financial industry
  - Payment Card Industry - Data Security Standard (PCI-DSS)
- Conclusions

# Timing System “Security Perimeter”


Unprotected PNT from the Sky


Network Firewall

# Common Vulnerabilities and Exposures (CVE) Update



**CVE Numbering Authorities (CNAs)**

Totals CNAs: 93 | Total Countries: 16

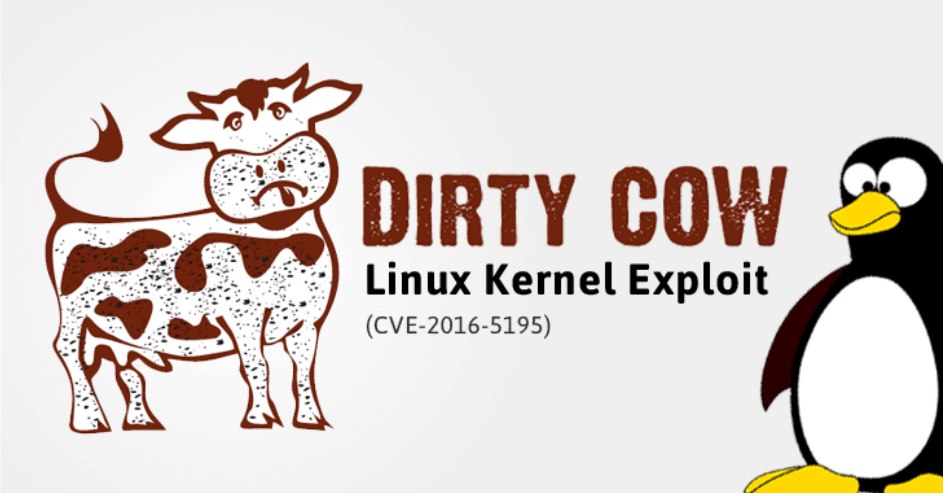
CNAs include vendors and projects, vulnerability researchers, national and industry CERTs, and bug bounty programs.

CNAs are how the CVE List is built. Every CVE Entry added to the list is assigned by a CNA.

- The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures
- CVE Numbering Authorities (CNAs) Assign and publish CVEs
- Funded by US DHS, and operated by Mitre Corporation
- Refer to https://cve.mitre.org/index.html

# Anatomy of a CVE

- The CVE system establishes a standard for reporting and tracking vulnerabilities
- Every CVE is given a unique number in the format “CVE-YEAR-NUMBER”
  - For example:  CVE-2019-1234
- CVEs are assigned a severity level from “None” to “Critical”
- Some famous CVEs are given names and even logos

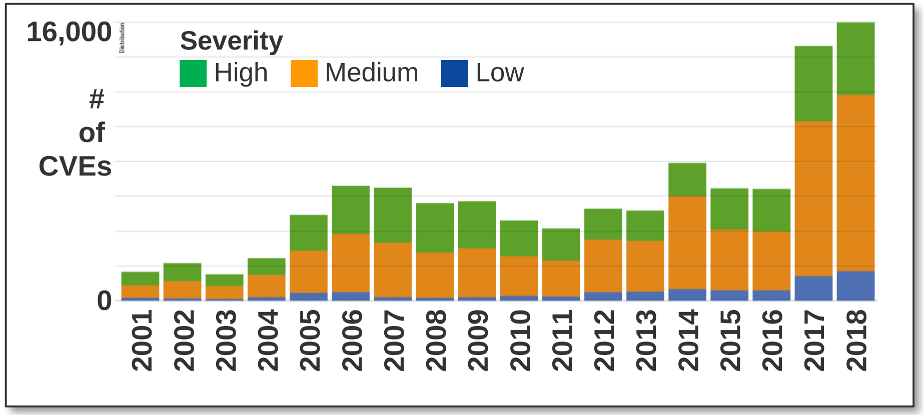


# Equifax Security Breach

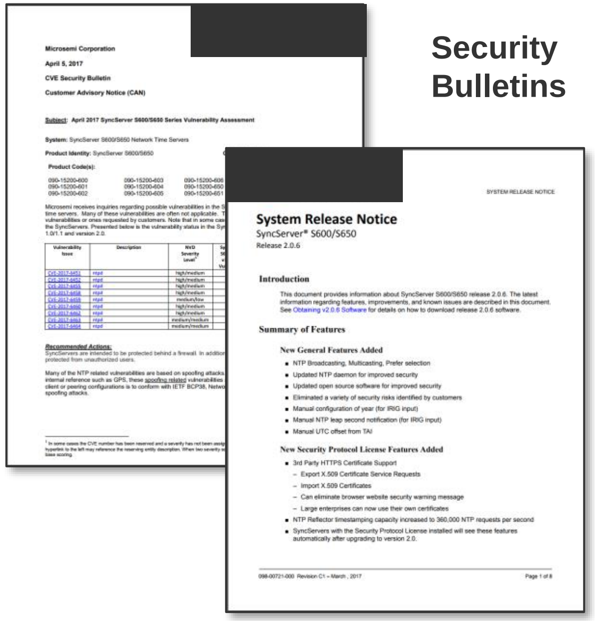
- 148 Million people impacted with stolen information including social security numbers
- Breach was traced to a single internet facing web server with down level SW
- Exploit was open and undetected for 76 days
- The vulnerability exploited was Apache Struts CVE-2017-5638

# CVE Exposures are Increasing

- Record number of CVEs documented in 2018



- CVE Activity
  - Investigated 86 possible CVEs*
  - Identified and mitigated 2 applicable CVEs
  - This is valuable to ALL customers



[redacted]

Microsemi Corporation

April 5, 2017

CVE Security Bulletin

Customer Advisory Notice (CAN)

Subject: April 2017 SyncServer S600/S650 Series Vulnerability Assessment

System: SyncServer S600/S650 Network Time Servers

Product Identity: SyncServer S600/S650

Product Code(s):

090-15200-600 090-15200-603 090-15200-606
090-15200-601 090-15200-604 090-15200-650
090-15200-602 090-15200-605 090-15200-651

Microsemi receives inquiries regarding possible vulnerabilities in the S
time servers. Many of these vulnerabilities are often not applicable. T
vulnerabilities or ones requested by customers. Note that in some cas
the SyncServers. Presented below is the vulnerability status in the Sy
1.0/1.1 and version 2.0.

| Vulnerability Issue | Description | NVD Severity Level[1] |
|---|---|---|
| CVE-2017-6451 | ntpd | high/medium |
| CVE-2017-6452 | ntpd | high/medium |
| CVE-2017-6455 | ntpd | high/medium |
| CVE-2017-6458 | ntpd | high/medium |
| CVE-2017-6459 | ntpd | medium/low |
| CVE-2017-6460 | ntpd | high/medium |
| CVE-2017-6462 | ntpd | high/medium |
| CVE-2017-6463 | ntpd | medium/medium |
| CVE-2017-6464 | ntpd | medium/medium |

***Recommended Actions:***
SyncServers are intended to be protected behind a firewall. In addition
protected from unauthorized users.

Many of the NTP related vulnerabilities are based on spoofing attacks
internal reference such as GPS, these spoofing related vulnerabilities
client or peering configurations is to conform with IETF BCP38, Netwo
spoofing attacks.

[1] In some cases the CVE number has been reserved and a severity has not been assig
hyperlink to the left may reference the reserving entity description. When two severity s
base scoring.

**Security Bulletins**

[redacted]

SYSTEM RELEASE NOTICE

## System Release Notice

SyncServer® S600/S650
Release 2.0.6

### Introduction

This document provides information about SyncServer S600/S650 release 2.0.6. The latest information regarding features, improvements, and known issues are described in this document. See Obtaining v2.0.6 Software for details on how to download release 2.0.6 software.

### Summary of Features

#### New General Features Added

- NTP Broadcasting, Multicasting, Prefer selection
- Updated NTP daemon for improved security
- Updated open source software for improved security
- Eliminated a variety of security risks identified by customers
- Manual configuration of year (for IRIG input)
- Manual NTP leap second notification (for IRIG input)
- Manual UTC offset from TAI

#### New Security Protocol License Features Added

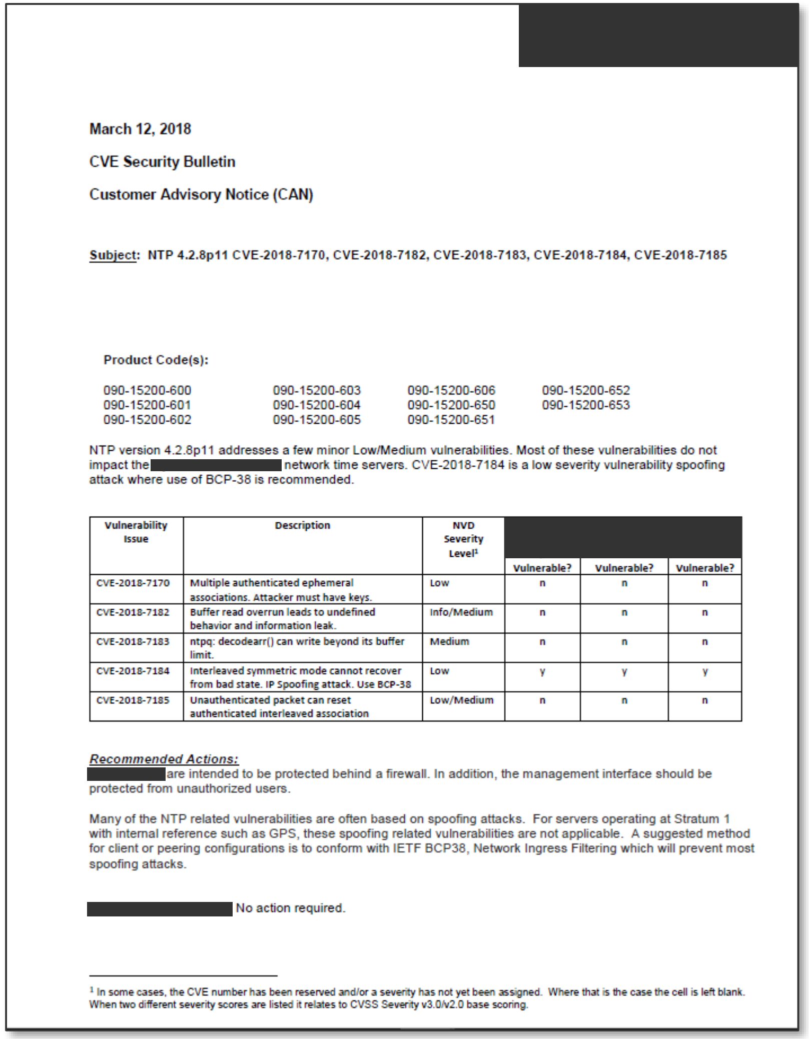
- 3rd Party HTTPS Certificate Support
  - Export X.509 Certificate Service Requests
  - Import X.509 Certificates
  - Can eliminate browser website security warning message
  - Large enterprises can now use their own certificates
- NTP Reflector timestamping capacity increased to 360,000 NTP requests per second
- SyncServers with the Security Protocol License installed will see these features automatically after upgrading to version 2.0.

098-00721-000 Revision C1 – March , 2017 Page 1 of 8

**System Release Notices (SRN)**

* CVE-2018-0739, CVE-2018-1087, CVE-2018-1118, CVE-2018-1120, CVE-2018-1130, CVE-2018-1283, CVE-2018-1301, CVE-2018-1302, CVE-2018-1303, CVE-2018-1312, CVE-2018-3620, CVE-2018-3639, CVE-2018-3646, CVE-2018-3665, CVE-2018-3693, CVE-2018-5750, CVE-2018-5803, CVE-2018-5953, CVE-2018-5995, CVE-2018-6412, CVE-2018-6554, CVE-2018-6555, CVE-2018-7182, CVE-2018-7170, CVE-2018-7182, CVE-2018-7183, CVE-2018-7184, CVE-2018-7185, CVE-2018-7754, CVE-2018-7755, CVE-2018-10322, CVE-2018-10323, CVE-2018-10675, CVE-2018-10840, CVE-2018-10853, CVE-2018-10872, CVE-2018-10876, CVE-2018-10877, CVE-2018-10878, CVE-2018-10879, CVE-2018-10880, CVE-2018-10881, CVE-2018-10882, CVE-2018-10883, CVE-2018-10901, CVE-2018-10902, CVE-2018-10938, CVE-2018-12232, VCE-2018-12233, CVE-2018-12327, CVE-2018-12633, CVE-2018-12714, CVE-2018-12904, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-13096, CVE-2018-13097, CVE-2018-13098, CVE-2018-13099, CVE-2018-13100, CVE-2018-13405, CVE-2018-13406, CVE-2018-13982, CVE-2018-14609, CVE-2018-14610, CVE-2018-14611, CVE-2018-14612, CVE-2018-14613, CVE-2018-14614, CVE-2018-14615, CVE-2018-14616, CVE-2018-14617, CVE-2018-14619, CVE-2018-14625, CVE-2018-14678, CVE-2018-14734, CVE-2018-15471, CVE-2018-15572, CVE-2018-15594, CVE-2018-16276, CVE-2018-16597, CVE-2018-16658, CVE-2018-17182, CVE-2018-18386, CVE-2018-1000204

# Security Bulletins



[redacted]

March 12, 2018

CVE Security Bulletin

Customer Advisory Notice (CAN)

<u>Subject</u>: NTP 4.2.8p11 CVE-2018-7170, CVE-2018-7182, CVE-2018-7183, CVE-2018-7184, CVE-2018-7185

Product Code(s):

| | | | |
|---|---|---|---|
| 090-15200-600 | 090-15200-603 | 090-15200-606 | 090-15200-652 |
| 090-15200-601 | 090-15200-604 | 090-15200-650 | 090-15200-653 |
| 090-15200-602 | 090-15200-605 | 090-15200-651 | |

NTP version 4.2.8p11 addresses a few minor Low/Medium vulnerabilities. Most of these vulnerabilities do not impact the [redacted] network time servers. CVE-2018-7184 is a low severity vulnerability spoofing attack where use of BCP-38 is recommended.

| Vulnerability Issue | Description | NVD Severity Level[1] | [redacted] | | |
|---|---|---|---|---|---|
| | | | Vulnerable? | Vulnerable? | Vulnerable? |
| CVE-2018-7170 | Multiple authenticated ephemeral associations. Attacker must have keys. | Low | n | n | n |
| CVE-2018-7182 | Buffer read overrun leads to undefined behavior and information leak. | Info/Medium | n | n | n |
| CVE-2018-7183 | ntpq: decodearr() can write beyond its buffer limit. | Medium | n | n | n |
| CVE-2018-7184 | Interleaved symmetric mode cannot recover from bad state. IP Spoofing attack. Use BCP-38 | Low | y | y | y |
| CVE-2018-7185 | Unauthenticated packet can reset authenticated interleaved association | Low/Medium | n | n | n |

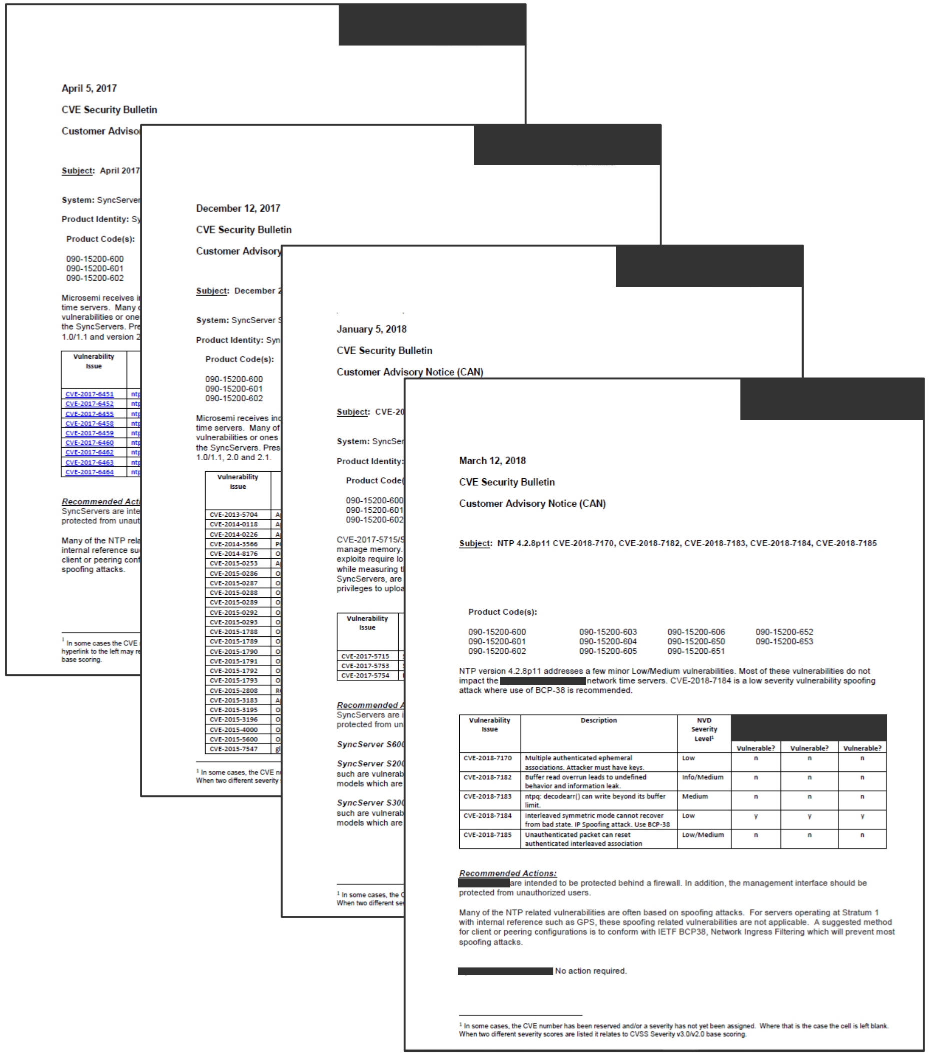
***<u>Recommended Actions:</u>***

[redacted] are intended to be protected behind a firewall. In addition, the management interface should be protected from unauthorized users.

Many of the NTP related vulnerabilities are often based on spoofing attacks. For servers operating at Stratum 1 with internal reference such as GPS, these spoofing related vulnerabilities are not applicable. A suggested method for client or peering configurations is to conform with IETF BCP38, Network Ingress Filtering which will prevent most spoofing attacks.

[redacted] No action required.

[1] In some cases, the CVE number has been reserved and/or a severity has not yet been assigned. Where that is the case the cell is left blank. When two different severity scores are listed it relates to CVSS Severity v3.0/v2.0 base scoring.



April 5, 2017

CVE Security Bulletin

December 12, 2017

CVE Security Bulletin

January 5, 2018

CVE Security Bulletin

Customer Advisory Notice (CAN)

March 12, 2018

CVE Security Bulletin

Customer Advisory Notice (CAN)

Subject: NTP 4.2.8p11 CVE-2018-7170, CVE-2018-7182, CVE-2018-7183, CVE-2018-7184, CVE-2018-7185

# Financial Services and Banking Requirements

Financial Services

- The financial services and banking industries take security very seriously
- It is very common for them to perform exhaustive security assessments on vendor equipment and demand fixes and enhancements as part of the equipment approval process
- A good example is the Payment Card Industry Data Security Standard (PCI-DSS)

# Payment Card Industry Data Security Standard (PCI-DSS)

- PCI DSS is an information security standard for organizations that handle branded credit cards from the major card companies
- Created to increase controls around cardholder data to reduce credit card fraud
- The PCI Data Security Standard specifies twelve requirements for compliance
- Requirement 10 covers tracking and monitoring all access to cardholder data and network resources, and includes specific requirement on the use of Network Time Protocol (NTP).

# PCI DSS Timing Requirements

Payment Card Industry (PCI)
**Data Security Standard**

**Requirements and Security Assessment Procedures**

**Version 3.2.1**
May 2018

- PCI DSS Requirements
  - Build and Maintain a secure Network and Systems
  - Protect Cardholder Data
  - Maintain a Vulnerability Management Program
  - Implement Strong Access Control Measures
  - Regularly Monitor and Test Networks
  - Maintain and Information Security Policy
- PCI DSS Requirement 10.4 Mandates Time Synchronization for all logs
  - All systems must synchronize their logs to centralized time servers
  - Only central time servers are allowed to receive time from external sources
  - External time sources must be based on TAI or UTC
  - If multiple centralized time servers are used, they must “peer” with each other to keep accurate time

# Conclusions

- A robust security perimeter is required for all Timing Systems used in critical infrastructures
- CVEs must be proactively monitored and addressed to close vulnerabilities
- Stringent financial services and banking requirements regarding security of timing infrastructure benefit all industries

# Thank you

Microsemi, a wholly owned subsidiary of Microchip Technology Inc. (Nasdaq: MCHP), offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; enterprise storage and communication solutions, security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Learn more at www.microsemi.com.

**Microsemi Headquarters**
One Enterprise, Aliso Viejo, CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
email: sales.support@microsemi.com
www.microsemi.com

Microsemi makes no warranty, representation, or guarantee regarding the information contained herein or the suitability of its products and services for any particular purpose, nor does Microsemi assume any liability whatsoever arising out of the application or use of any product or circuit. The products sold hereunder and any other products sold by Microsemi have been subject to limited testing and should not be used in conjunction with mission-critical equipment or applications. Any performance specifications are believed to be reliable but are not verified, and Buyer must conduct and complete all performance and other testing of the products, alone and together with, or installed in, any end-products. Buyer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is the Buyer's responsibility to independently determine suitability of any products and to test and verify the same. The information provided by Microsemi hereunder is provided "as is, where is" and with all faults, and the entire risk associated with such information is entirely with the Buyer. Microsemi does not grant, explicitly or implicitly, to any party any patent rights, licenses, or any other IP rights, whether with regard to such information itself or anything described by such information. Information provided in this document is proprietary to Microsemi, and Microsemi reserves the right to make any changes to the information in this document or to any products and services at any time without notice.