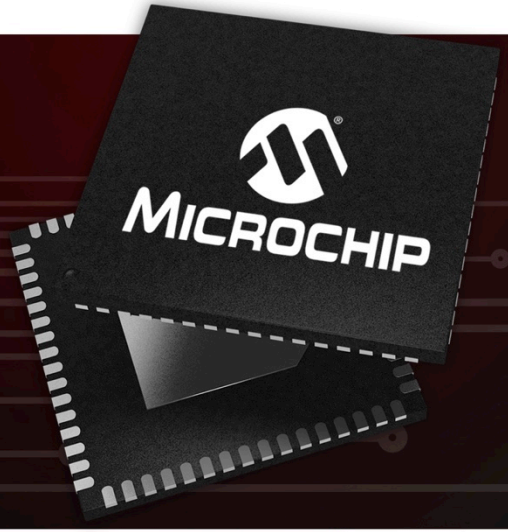
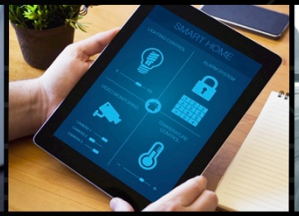
MICROCHIP



A Leading Provider of Microcontroller, Security, Mixed-Signal, Analog & Flash-IP Solutions



Security of Timing Infrastructure - Network Based Threats and CVEs

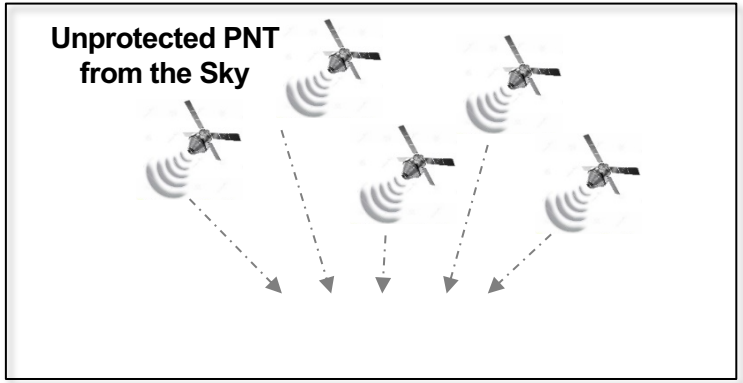
Barry Dropping

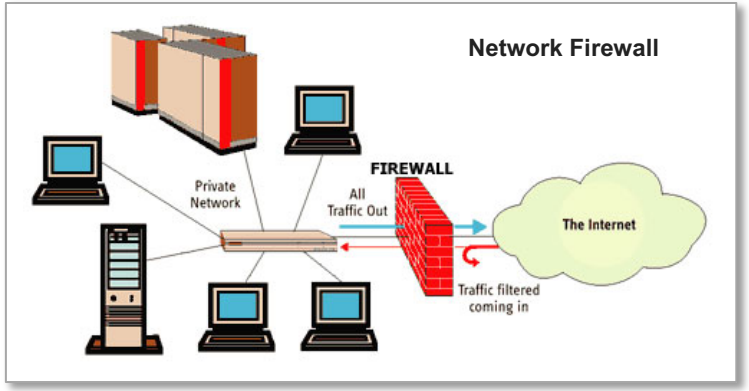
November 2019

Agenda

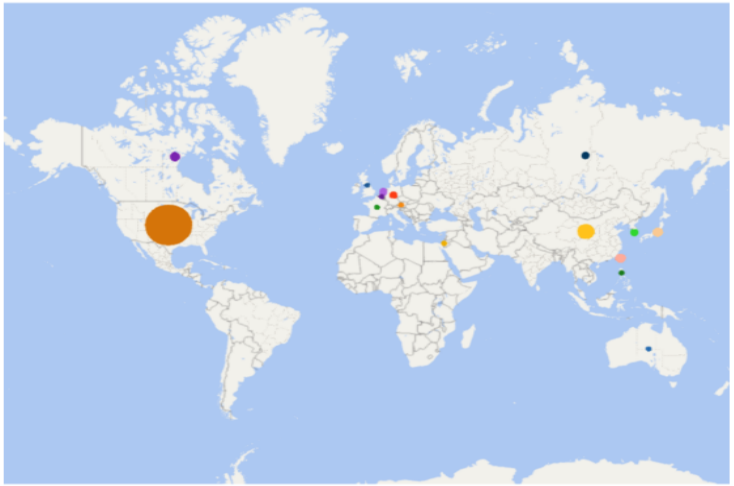
- **“Security Perimeter” of network based time servers**
- **Common Vulnerabilities and Exposures (CVE) Update**
- **Best practices in addressing CVEs**
- **Additional security requirement in the financial industry**
  - Payment Card Industry - Data Security Standard (PCI-DSS)
- **Conclusions**

Timing System "Security Perimeter"





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

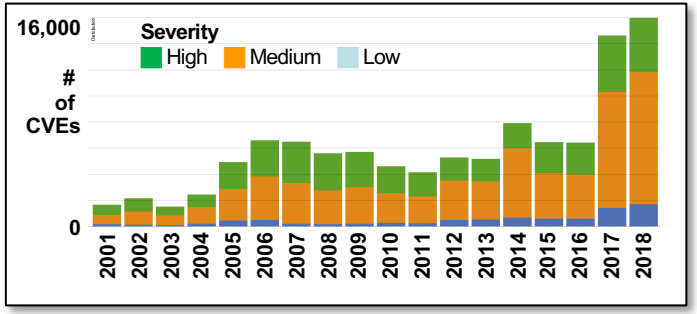
- **The CVE system establishes a standard for reporting and tracking vulnerabilities**
- **Every CVE is given a unique number in the format "CVE-YEAR-NUMBER"**
  - For example: CVE-2019-1234
- **CVEs are assigned a severity level from "None" to "Critical"**
- **Some famous CVEs are given names and even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

Equifax Security Breach

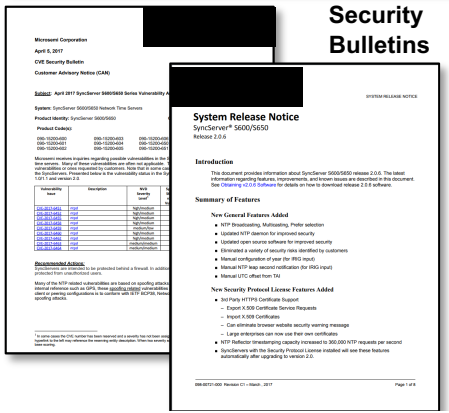
- 148 Million people impacted with stolen information including social security numbers
- Breach was traced to a single internet facing web server with down level SW
- Exploit was open and undetected for 76 days
- The vulnerability exploited was Apache Struts CVE-2017-5638

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



Security Bulletins

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

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

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

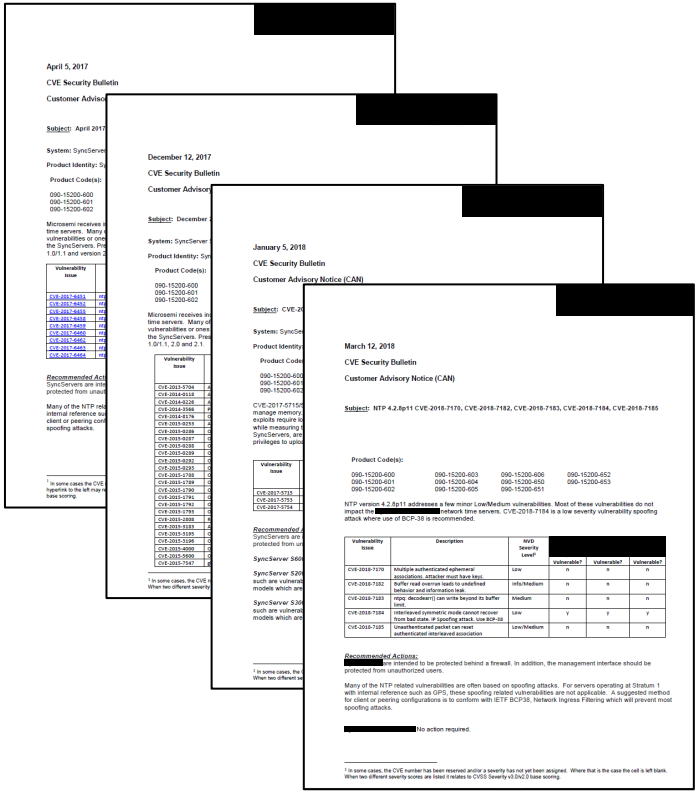
Recommended Actions:

[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.



Financial Services and Banking Requirements

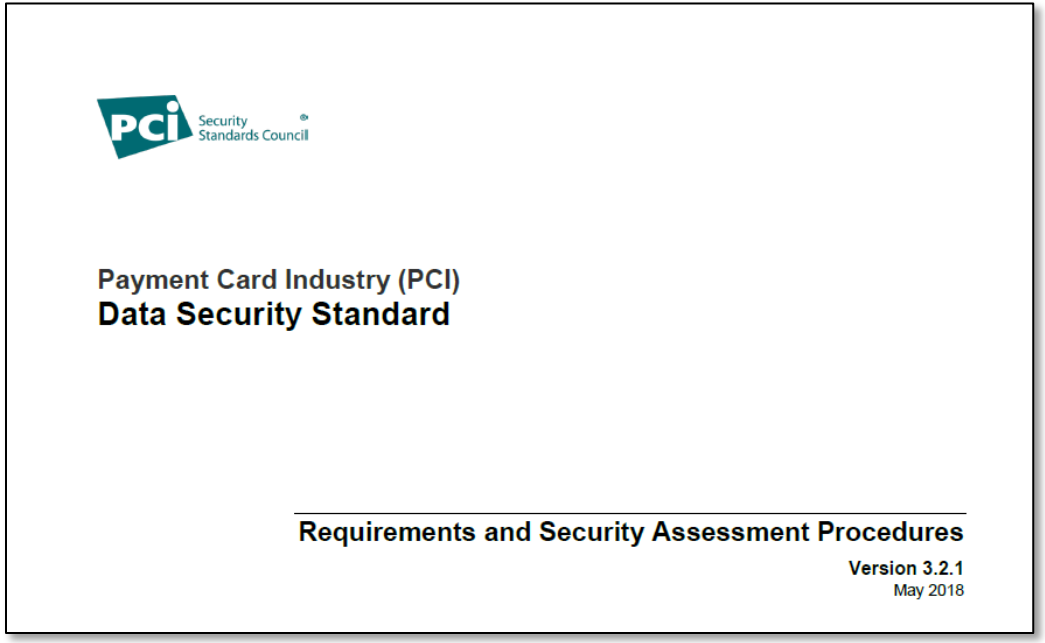
Financial Services

- **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