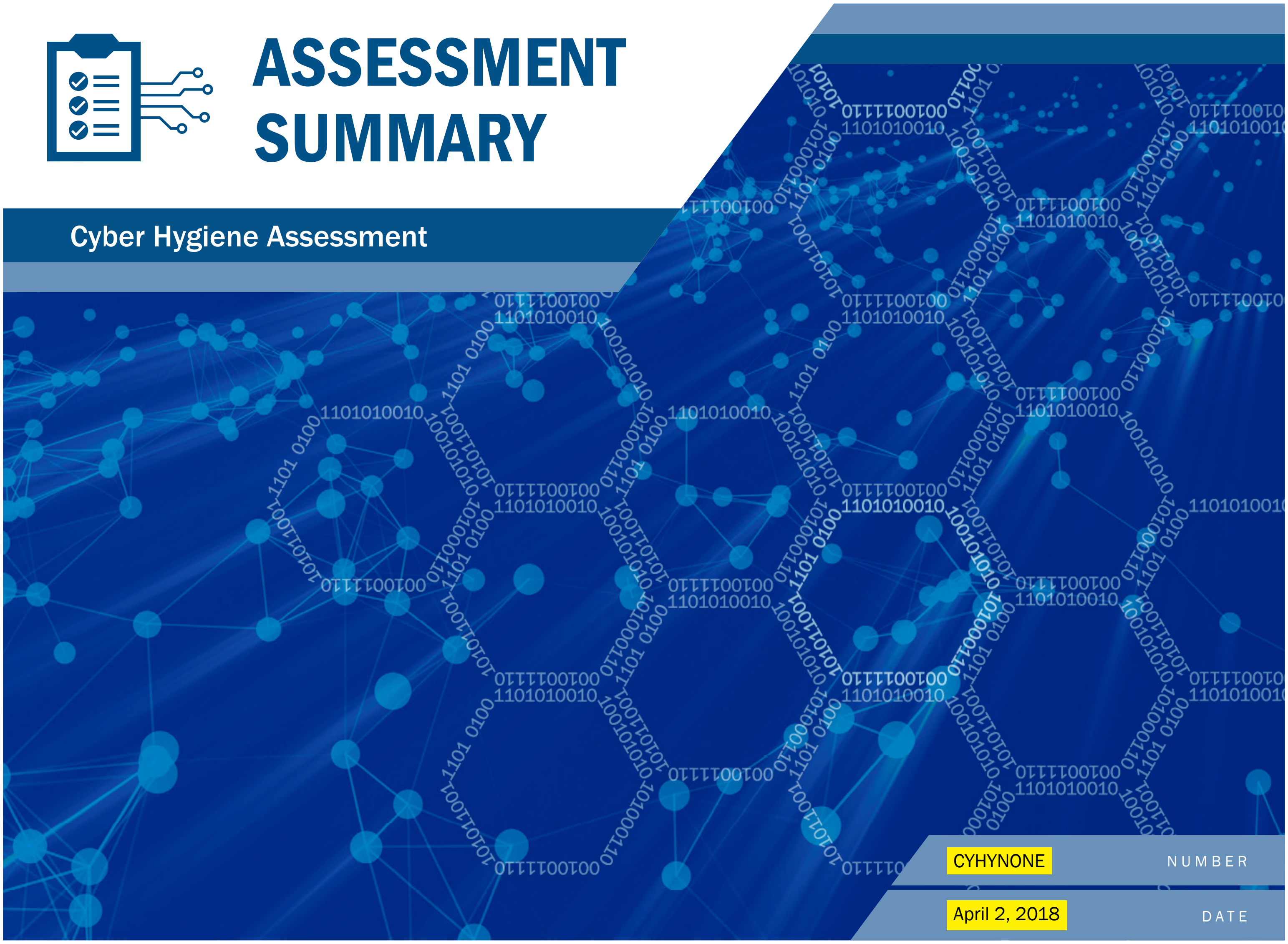
ASSESSMENT SUMMARY

Cyber Hygiene Assessment



CYHYNONE	NUMBER
April 2, 2018	DATE

Cyber Hygiene Assessment

Sample Organization

NCCIC

Contents

List of Figures

List of Tables

1 How To Use This Report

Welcome to your Cyber Hygiene (CyHy) report. This document aims to be a comprehensive weekly snapshot of known vulnerabilities detected on Internet-facing hosts for Sample Organization (SAMPLE).

You may wonder what you're supposed to do with all this information. While it's not our intent to prescribe to you a particular process for remediating vulnerabilities, we hope you'll use this report to strengthen your security posture. Here's a basic flow:

1. Review the Cyber Hygiene Report Card for a high-level overview. This section gives a quick comparison of the problems we find week to week. If this is your first report, you should note that the Report Card will initially lack historical data to make comparisons against, though that data will exist in your next report.
2. See Appendix A: Vulnerability Summary for a list of unique vulnerabilities across all the systems we detect problems with. Appendix C: Detailed Findings and Recommended Mitigations by Vulnerability provides more information about each vulnerability and all the hosts that we detect are susceptible to a given vulnerability. You should focus on those vulnerabilities rated with the greatest severity, as well as those that impact your high-value assets, but don't ignore the medium or low vulnerabilities. Recognize that a vulnerability's rating tends to get worse with time.
3. If this report is not your first, review Appendix B: Vulnerability Changes Since Last Report for a breakdown of all the changes we detected in your scope in the last week.
4. If you've patched a vulnerability since your last report, verify it's listed here. If it's not present, there may still be an issue. It may also be possible that the issue was fixed after our latest scan, which was on April 2, 2018.
5. For additional analysis, see Appendix G: Attachments, which provides Comma-Separated Values (CSV) files for all findings, services, hosts, and the scope that we scan.

You should be aware that Cyber Hygiene does not scan your entire scope (all of the addresses your organization has sent us) every week, but does attempt to scan every host each week. For an explanation of how CyHy works, see the Methodology section.

As you review the report, you may have additional questions. Check out the answers we provide in the Frequently Asked Questions section. If you have any additional questions, email us at ncats@hq.dhs.gov.

1.1 SAMPLE Points of Contact

SAMPLE has defined the following points-of-contact for Cyber Hygiene activities; if present, reports are emailed solely to distribution lists. If you receive this report through a distribution list, Department of Homeland Security (DHS) requests that you funnel your request through your technical POC(s).

Type	Name	Email Address	Phone Number
Technical	Technical POC 1	tech_poc_1@sample.org	555-555-1111
Technical	Technical POC 2	tech_poc_2@sample.org	555-555-2222
Distribution List	Distro POC 1	distro_poc_1@sample.org	

CYBER HYGIENE REPORT CARD

HIGH LEVEL FINDINGS

ADDRESSES OWNED

293,005 ↔

no change

ADDRESSES SCANNED

293,005 ↔

no change

100% of addresses scanned

LATEST SCANS

Addresses: December 5, 2017 — April 4, 2018
Vulnerabilities: March 28, 2018 — April 4, 2018

HOSTS

3,986

38 decrease

VULNERABLE HOSTS

393

44 decrease

10% of hosts vulnerable

VULNERABILITIES

1,159

192 decrease

SERVICES

8,724

196 decrease

VULNERABILITIES

🟥 CRITICAL

10

2 resolved
0 new

🟧 HIGH

4 ↔

1 resolved
1 new

🟨 MEDIUM

1,044

258 resolved
108 new

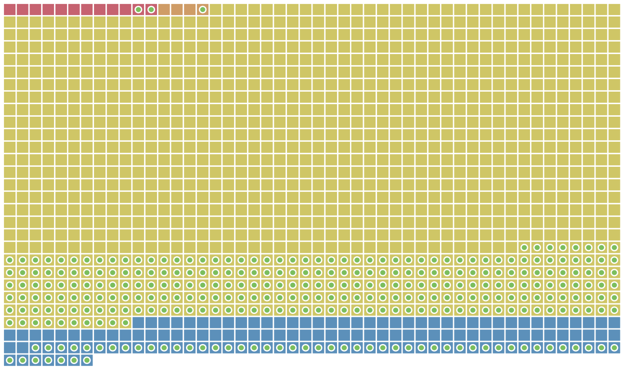
🟦 LOW

101

53 resolved
13 new

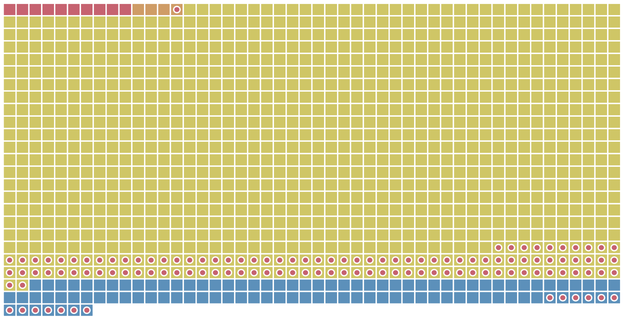
PREVIOUS REPORT

● resolved



CURRENT REPORT

● new



VULNERABILITY RESPONSE TIME (since April 2, 2017)

	🟥 CRITICAL		🟧 HIGH		🟨 MEDIUM		🟦 LOW	
	Median	Maximum	Median	Maximum	Median	Maximum	Median	Maximum
DAYS TO MITIGATE	8	86	27	1,601	158	1,952	37	1,517
DAYS CURRENTLY ACTIVE	28	29	54	210	307	1,952	29	1,622

3 Executive Summary

This report provides the results of a DHS / National Cybersecurity Assessments and Technical Services (NCATS) CyHy assessment of SAMPLE conducted from December 5, 2017 at 15:54 UTC through April 2, 2018 at 03:53 UTC. The Cyber Hygiene assessment includes network mapping and vulnerability scanning for Internet-accessible SAMPLE hosts. This report is intended to provide SAMPLE with enhanced understanding of their cyber posture and to promote a secure and resilient Information Technology (IT) infrastructure across SAMPLE's Internet-accessible networks and hosts.

For this reporting period, a total of 3,986 hosts were identified out of the 293,005 addresses provided to NCATS. The scanning revealed 1,159 total potential vulnerabilities on 393 vulnerable hosts, 10% of all SAMPLE hosts. 143 distinct open ports, 67 distinct services, and 132 operating systems were detected.

63 distinct types of potential vulnerabilities (3 critical, 3 high, 43 medium, and 14 low) were detected, as shown in Table 1. The vulnerabilities that were detected most frequently on SAMPLE hosts are displayed in Figure 1.

SAMPLE should review the potential vulnerabilities detected and report any false positives back to NCATS so they can be excluded from future reports. Please refer to Appendix A: Vulnerability Summary for an illustration of the breakdown of vulnerability occurrences over time.

Severity	Distinct Vulnerabilities		Total Vulnerabilities	
Critical	5%	3	1%	10
High	5%	3	0%	4
Medium	68%	43	90%	1,044
Low	22%	14	9%	101
Total		63		1,159

Table 1: Number of Vulnerabilities by Severity Level

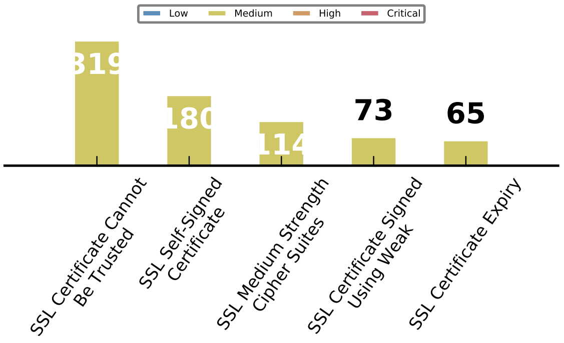


Figure 1: Top Vulnerabilities by Occurrence

Additionally, the top high-risk hosts and top risk-based vulnerabilities are displayed in Figure 2 and Figure 3. For more information about these risk calculations, refer to Table 8: Risk Rating System.

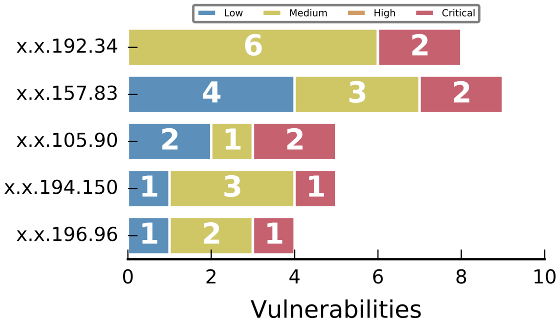


Figure 2: Top High-Risk Hosts

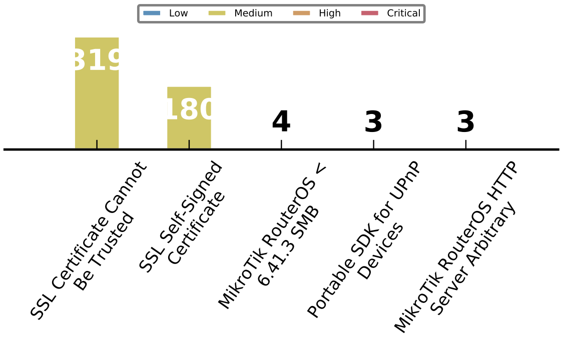


Figure 3: Top Risk-Based Vulnerabilities

The most frequently detected operating systems and services for SAMPLE are displayed in Table 2 and Table 3 respectively.

Operating System	Detections	
unknown	70.3%	3,157
OpenBSD 4.0	6.1%	272
F5 BIG-IP Edge Gateway	4.3%	195
FreeBSD 6.2-RELEASE	3.7%	168
OpenBSD 4.3	2.6%	116
Other	12.9%	580

Table 2: Top Operating Systems Detected

Service	Detections	
domain	0.3%	25
jetdirect	0.1%	8
pop3	0.0%	2
gw	0.0%	1
xmpp	0.0%	1
Other	99.6%	8,657

Table 3: Top Services Detected

The next two figures illustrate how quickly SAMPLE responds to vulnerabilities that have been identified. Figure 4 shows how long it has taken SAMPLE to mitigate vulnerabilities of each severity level (for vulnerabilities mitigated since April 2, 2017), while Figure 5 shows the median ages of current active vulnerabilities. Vulnerability age is based on the initial detection date by CyHy.

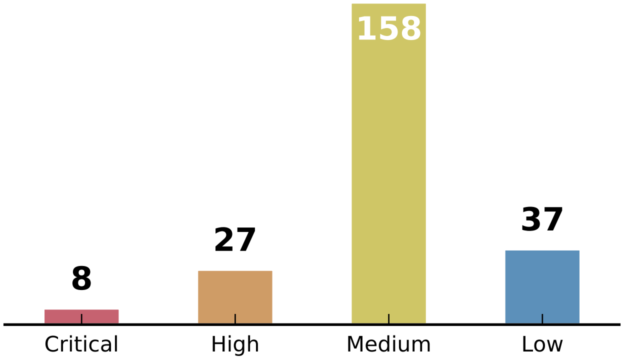


Figure 4: Median Time in Days to Mitigate Vulnerabilities

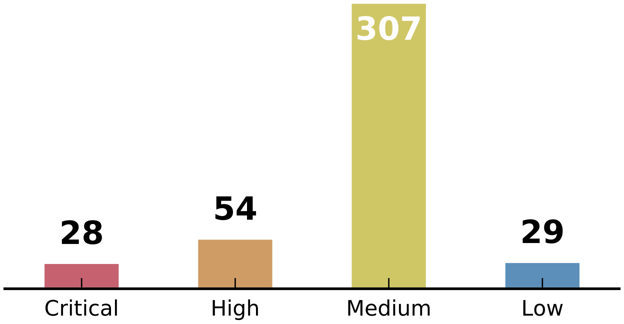


Figure 5: Median Age in Days of Active Vulnerabilities

Figure 6 displays the number of active critical vulnerabilities that were less than 30 days old and more than 30 days old, as of the date indicated on the graph. Vulnerability age is based on the initial detection date by CyHy.

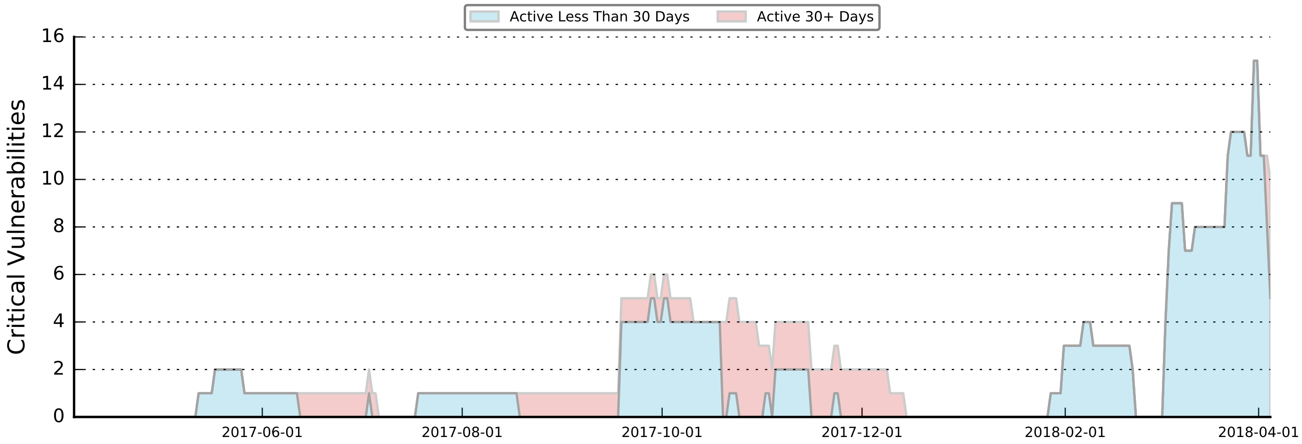


Figure 6: Critical Vulnerability Age Over Time

Figure 7 and Table 4 provide an age breakdown of every currently active critical vulnerability for SAMPLE.

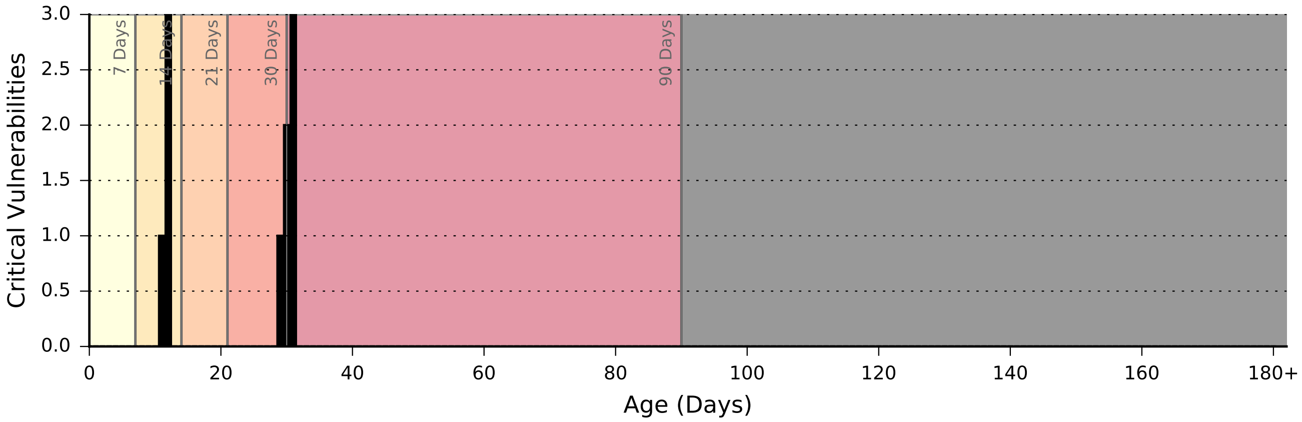


Figure 7: Active Critical Vulnerability Age

	0-7 Days	7-14 Days	14-21 Days	21-30 Days	30-90 Days	90+ Days
Active Critical Vulnerabilities	0	4	0	1	5	0

Table 4: Active Critical Vulnerability Age Summary

4 Sub-Organization Summary

This section shows the key CyHy metrics for each sub-organization within SAMPLE. A CSV with this data can be found in Appendix G: Attachments.

Org	Addresses		Hosts		Vulnerabilities Detected				Services	Median Days To Mitigate				Median Days Currently Active			
Name	Owned	Scanned	Detected	Vulnerable	Critical	High	Med	Low	Detected	Critical	High	Med	Low	Critical	High	Med	Low
SUB_ORG	9,721	100%	3,360	97 (3%)	0	0	248	8	6,796	0	189	214	256	0	0	336	1,349
SUB_ORG	65,610	100%	79	8 (10%)	0	0	18	0	196	83	15	55	57	0	0	583	0
SUB_ORG	77,800	100%	85	44 (52%)	0	4	133	13	187	11	55	110	164	0	54	207	354
SUB_ORG	827	100%	1	0 (0%)	0	0	0	0	1	0	0	100	0	0	0	0	0
SUB_ORG	123	100%	115	79 (69%)	0	0	224	16	396	1	2	179	161	0	0	478	1,272
SUB_ORG	448	100%	93	64 (69%)	10	0	139	54	400	12	31	21	17	28	0	28	28
SUB_ORG	2,125	100%	23	12 (52%)	0	0	21	1	55	0	0	227	107	0	0	414	348
SUB_ORG	272	100%	1	1 (100%)	0	0	1	0	1	0	16	16	0	0	0	394	0
SUB_ORG	28	100%	18	9 (50%)	0	0	34	0	48	0	1	340	119	0	0	478	0
SUB_ORG	520	100%	129	57 (44%)	0	0	179	4	512	4	39	234	219	0	0	479	10
SUB_ORG	6	100%	6	5 (83%)	0	0	8	0	19	0	0	147	64	0	0	449	0
SUB_ORG	134,877	100%	64	12 (19%)	0	0	29	4	99	0	108	272	145	0	0	339	214
SUB_ORG	648	100%	12	5 (42%)	0	0	10	1	14	10	0	59	115	0	0	214	214
SAMPLE Total	293,005	100%	3,986	393 (10%)	10	4	1,044	101	8,724	8	27	158	37	28	54	307	29

5 Methodology

5.1 Background

The NCATS team conducted a Cyber Hygiene assessment of SAMPLE's Internet-facing networks and hosts from December 5, 2017 at 15:54 UTC through April 2, 2018 at 03:53 UTC. This report provides result summaries and detailed findings of the CyHy assessment activity for SAMPLE and its associated sub-organizations. All scan results are included in Appendix G: Attachments as CSV files.

Cyber Hygiene is intended to improve your security posture by proactively identifying and reporting on vulnerabilities and configuration issues present on Internet-facing systems before those vulnerabilities can be exploited.

Cyber Hygiene is a service of NCATS, organized under the DHS National Protection and Programs Directorate (NPPD), Office of Cybersecurity and Communications (CS&C), National Cybersecurity and Communications Integration Center (NCCIC).

DHS began Cyber Hygiene in January 2012 to assess, on a recurring basis, the "health" of unclassified federal civilian networks accessible via the Internet. Since then, the program has grown to provide a persistent scanning service to federal, state, local, tribal, and territorial governments and private sector organizations.

Upon submission of an Acceptance Letter, SAMPLE provided NCATS with their public network address information. SAMPLE and NCATS agreed on any time restrictions which would be imposed on the scanning activity.

5.2 Process

All Cyber Hygiene scanning activity originates from the **64.69.57.0/24** network.

CyHy uses a combination of scanning services for testing:

- Network Mapping
- Vulnerability Scanning

Network Mapping

Using Nmap [https://nmap.org], we attempt to determine what hosts are available, identify what services (application name and version) those hosts are offering, and what Operating System (OS) versions they are running. We first scan the most commonly detected 1,000 Transmission Control Protocol (TCP) ports of the addresses you've submitted to us to get a quick understanding of the active/dark landscape. An address that has a least one port open/listening service is considered a *host* and is then fully port-scanned (TCP) and included in the vulnerability scan. For the purposes of this report, *tcpwrapped* ports are not considered to be open; for more information on tcpwrapped ports, refer to the Frequently Asked Questions section.

If no services are detected in the most common 1,000 ports on a given Internet Protocol (IP) address, that address is considered "dark" in CyHy and will be re-scanned after at least 90 days to check for change. Addresses marked dark are not included in the host count of the weekly report. Understand that CyHy is not attempting to make a judgment call about why an address is unresponsive. If there's not a port open, it's not a *host* in the language of CyHy.

Vulnerability Scanning

Using Nessus, a commercial vulnerability scanner, each host is evaluated against a library of vulnerabilities that an Internet-based actor could exploit. Vulnerabilities are reported with a severity of critical, high, medium, or low to facilitate prioritization of remediation efforts. We enable all Nessus Plugins [https://www.tenable.com/plugins/] except those in the "Denial of Service" family.

Scanning Frequency

Scanning occurs continuously between each weekly report. All hosts are scanned for vulnerabilities at least once every two weeks; hosts with vulnerabilities are scanned more frequently.

Cyber Hygiene's scan prioritization is as follows:

- Addresses with no running services detected (dark space) are rescanned after at least 90 days.
- Hosts with no vulnerabilities detected are rescanned every 7 days.
- Hosts with low-severity vulnerabilities are rescanned every 6 days.
- Hosts with medium-severity vulnerabilities are rescanned every 4 days.
- Hosts with high-severity vulnerabilities are rescanned every 24 hours.
- Hosts with critical-severity vulnerabilities are rescanned every 12 hours.

You should understand that a single host may have multiple vulnerabilities of varying severity, which impacts the frequency that the host is scanned.

To be clear, it is not the case that we scan your entire address scope for vulnerabilities each week (unless each address you've provided to us has a responsive host). It is the case, though, that each host will get vulnerability scanned at least once per week.

Recurring Vulnerabilities

After you've remediated a vulnerability (and it remains resolved for a period of 90 days), the host's scan priority will drop. This approach allows the NCATS team to focus on the areas of importance and give more attention to the hosts that need it.

Vulnerabilities are assigned an age in order to track timeliness of remediation. Vulnerability age is determined by when it was first detected on a host, not from when it first appeared on a report. As scanning occurs continuously between weekly reports, it is possible to have "new" vulnerabilities appear on a report that are already days old. It is also possible for a vulnerability to fluctuate between being detected and not detected during mid-week scans and then at a future time appear in a report as many days old. If a mitigated vulnerability is re-detected less than 90 days after the date of non-detection, it will be considered to be the same vulnerability with the same "initial detection date" as previously recorded. If it is re-detected more than 90 days after the date of non-detection, it will be treated as a new vulnerability with a new "initial detection date".

Vulnerability Scoring

The Nessus vulnerability scanner references the National Vulnerability Database (NVD) [https://nvd.nist.gov/] for its vulnerability information. The NVD provides CVSS scores for many known vulnerabilities. In particular, NVD supports the CVSS version standard for all Common Vulnerabilities and Exposures (CVE) vulnerabilities.

The CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. The NVD uses severity rankings of “Low,” “Medium,” and “High” in addition to the numeric CVSS scores, but these qualitative rankings are simply mapped from the numeric CVSS base scores:

- Vulnerabilities are labeled “Low” severity if they have a CVSS base score of 0.0-3.9.
- Vulnerabilities will be labeled “Medium” severity if they have a base CVSS score of 4.0-6.9.
- Vulnerabilities will be labeled “High” severity if they have a CVSS base score of 7.0-10.0.

Nessus has a “critical” rating which it uses for CVSS 10 vulnerabilities. Where the NVD has not provided a CVE severity rating, the Nessus scanner relies on its own rankings.

What’s In The Report?

Though Cyber Hygiene initiates multiple scans between reports, *only the latest scan data for each host is used to determine current vulnerability*. This is the data that appears in the main body of the report and in Appendix A: Vulnerability Summary, Appendix B.2: New Vulnerabilities Detected and Appendix B.3: Re-Detected (Previously-Mitigated) Vulnerabilities.

If a vulnerability was detected since that last report (e.g., it wasn’t in the previous report’s findings, though CyHy saw it mid-week) but it was not in the latest scan, we include it in Appendix B.4: Recently-Detected Vulnerabilities.

If a vulnerability that was previously reported to you is no longer detected by the latest scan, the vulnerability and host will be listed in Appendix B.1: Mitigated Vulnerabilities.

We encourage you to validate the status of vulnerabilities in both Appendix B.1: Mitigated Vulnerabilities and Appendix B.4: Recently-Detected Vulnerabilities against your change control register. This will help to ensure that the vulnerability we detected has actually been remediated and is not simply unresponsive to our scans.

6 Approximate Host Locations

The map below shows the approximate locations of detected hosts as listed in a geo-location database. This map is provided as a tool to identify hosts that may have been mistakenly added in to, or removed from scope. The map is scaled to include all known SAMPLE host locations.

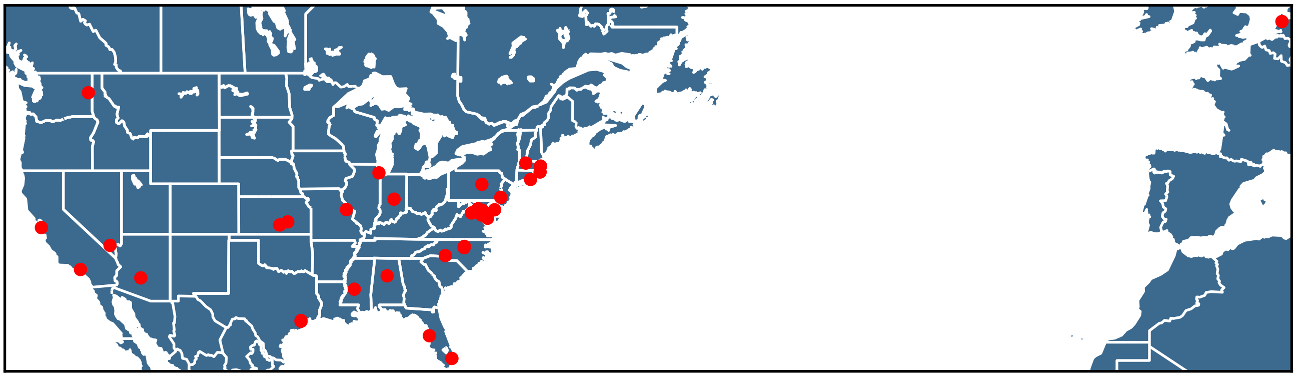


Figure 8: Approximate Host Locations

7 Vulnerability Scan Results

For this period, CyHy detected 1,159 occurrences of 63 distinct vulnerabilities (10 critical, 4 high, 1,044 medium, and 101 low). SAMPLE should review the vulnerabilities detected and report any false positives back to NCATS so these can be excluded from future reports (see the Frequently Asked Questions section for more about false positives).

The scanning detected 393 vulnerable hosts—364 hosts with one to five vulnerabilities were identified; 24 hosts had between six and nine vulnerabilities; 4 hosts had ten or more vulnerabilities identified.

Severity	Distinct Vulnerabilities		Total Vulnerabilities	
Critical	5%	3	1%	10
High	5%	3	0%	4
Medium	68%	43	90%	1,044
Low	22%	14	9%	101
Total		63		1,159

Table 5: Number of Vulnerabilities by Severity Level

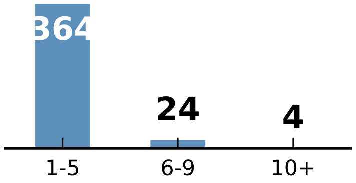


Figure 9: Vulnerability Count per Host

The CVSS scores for all active vulnerabilities can be found in Figure 10.

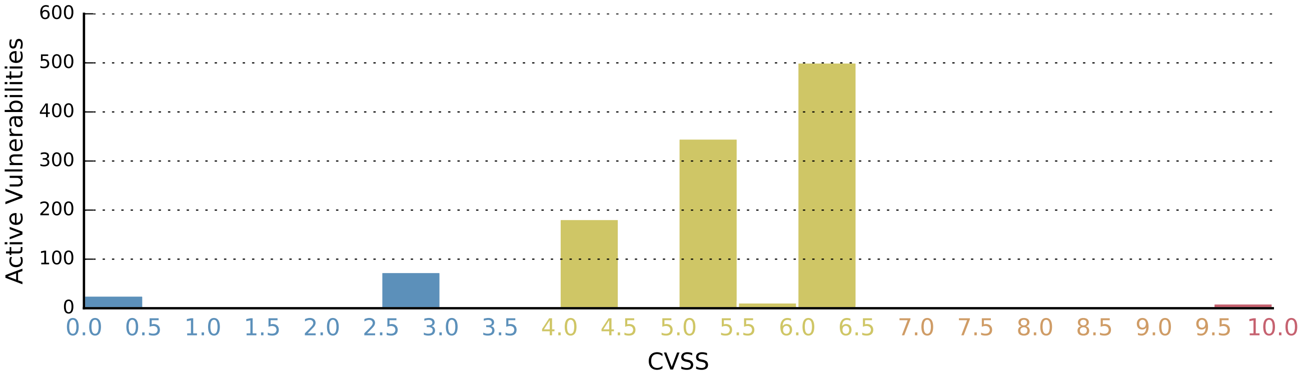


Figure 10: CVSS Histogram for Active Vulnerabilities

The top vulnerabilities according to CVSS score are represented in Table 6.

Vulnerability Name	Severity	Hosts	CVSS Score
MikroTik RouterOS < 6.41.3 SMB Buffer Overflow	Critical	4	10.0
MikroTik RouterOS HTTP Server Arbitrary Write RCE (ChimayRed)	Critical	3	10.0
Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE	Critical	3	10.0
PHP 5.6.x < 5.6.34 Stack Buffer Overflow	High	2	7.5
FTP Privileged Port Bounce Scan	High	1	7.5
SNMP Agent Default Community Name (public)	High	1	7.5
Apache Tomcat Default Files	Medium	2	6.8
AXIS gSOAP Message Handling RCE (ACV-116267) (Devil's Ivy)	Medium	1	6.8
SSL Certificate Cannot Be Trusted	Medium	319	6.4
SSL Self-Signed Certificate	Medium	180	6.4

Table 6: Top Vulnerabilities by CVSS

A complete list of distinct vulnerabilities detected, including severity level and number of hosts having the vulnerability can be found in Appendix A: Vulnerability Summary. Full details on every detected vulnerability can be found in Appendix C: Detailed Findings and Recommended Mitigations by Vulnerability. Every critical and high finding detected, along with the hosts that have these findings, are listed in Appendix D: Critical and High Vulnerability Mitigations by IP Address.

The top high-risk hosts are identified in Table 7 by combining the total number of vulnerabilities, the severity of the vulnerabilities, and a weighted CVSS score for vulnerabilities detected. For more information on the formula, please refer to Table 8: Risk Rating System.

IP Address	Critical	High	Medium	Low	Total
x.x.192.34	2	0	6	0	8
x.x.157.83	2	0	3	4	9
x.x.105.90	2	0	1	2	5
x.x.194.150	1	0	3	1	5
x.x.196.96	1	0	2	1	4
x.x.196.200	1	0	2	1	4
x.x.236.156	1	0	0	3	4
x.x.124.231	0	2	10	2	14
x.x.59.83	0	0	9	1	10
x.x.124.236	0	1	9	1	11

Table 7: Top Hosts by Weighted Risk

The Risk Rating System (RRS) emphasizes higher-rated CVSS scores to ensure that hosts with a large number of lower-risk vulnerabilities do not outweigh hosts with a smaller number of high-risk vulnerabilities, while ensuring that hosts with an extreme number of low-risk vulnerabilities are not overshadowed by hosts with a single higher-risk issue. The RRS also ensures that hosts with a significant number of high-risk vulnerabilities will not be overshadowed by a host with only a single critical vulnerability.

Table 8 illustrates the base and weighted CVSS scores and shows the equivalent number of lower-risk vulnerabilities to weigh evenly with a single critical (CVSS score of 10) vulnerability.

Base CVSS Score	Weighted CVSS Score	Equivalent to CVSS Score 10
1.0	1×10^{-06}	10,000,000.0
2.0	0.000,128	78,125.0
3.0	0.002,187	4,572.47
4.0	0.016,384	610.35
5.0	0.078,125	128.0
6.0	0.279,936	35.72
7.0	0.823,543	12.14
8.0	2.097,152	4.77
9.0	4.782,969	2.09
10.0	10.0	1.0

Table 8: Risk Rating System

As an example, a host having 400 vulnerabilities with a base CVSS score of 1.0 would get a weighted RRS score of 4×10^{-04}, which is considered lower-risk than a host with a single critical vulnerability (RRS score of 10.0). Similarly, a host having 4 vulnerabilities with a base CVSS score of 8 would get a RRS score of 8.39 and still be considered a lower risk than a host with a single critical vulnerability (RRS score of 10.0).

8 Results Trending

To help decision-makers, this section provides a comparison of the current data against similar CyHy scans conducted over time.

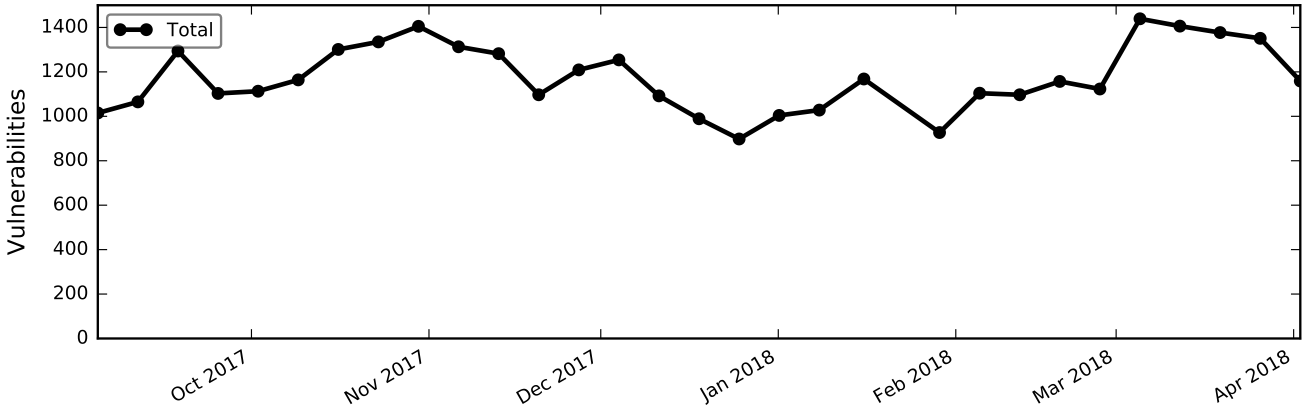


Figure 11: Total Active Vulnerabilities Over Time

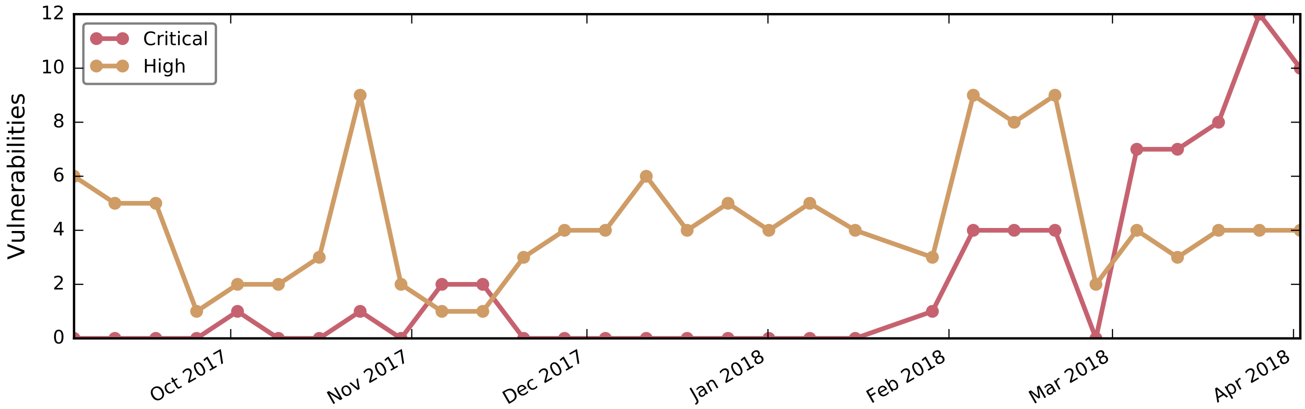


Figure 12: Active Critical and High Vulnerabilities Over Time

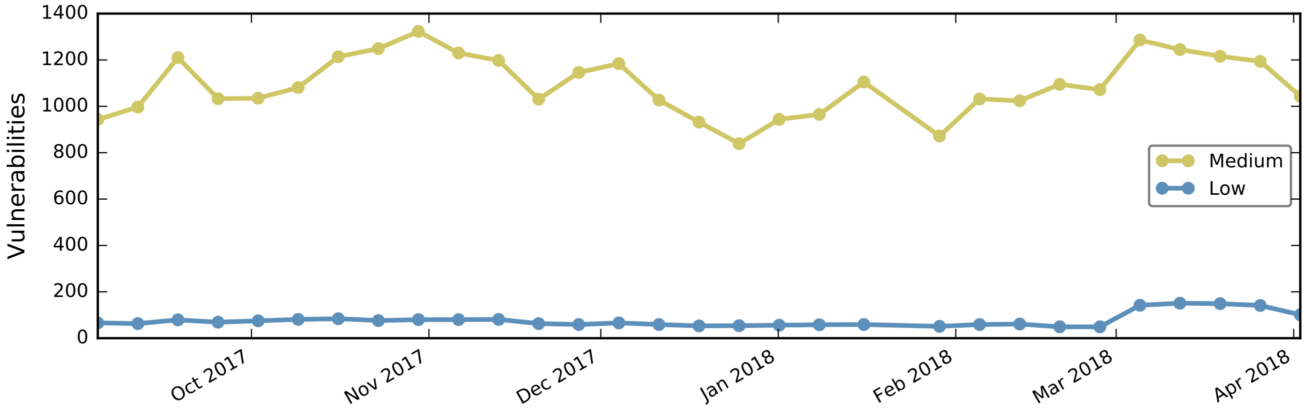


Figure 13: Active Medium and Low Vulnerabilities Over Time

SAMPLE vulnerability profile over time, reporting on the total hosts detected, number of hosts with vulnerabilities, number of distinct services, and the number of distinct vulnerabilities detected can be found in Figure 14, Figure 15, and Figure 16 respectively.

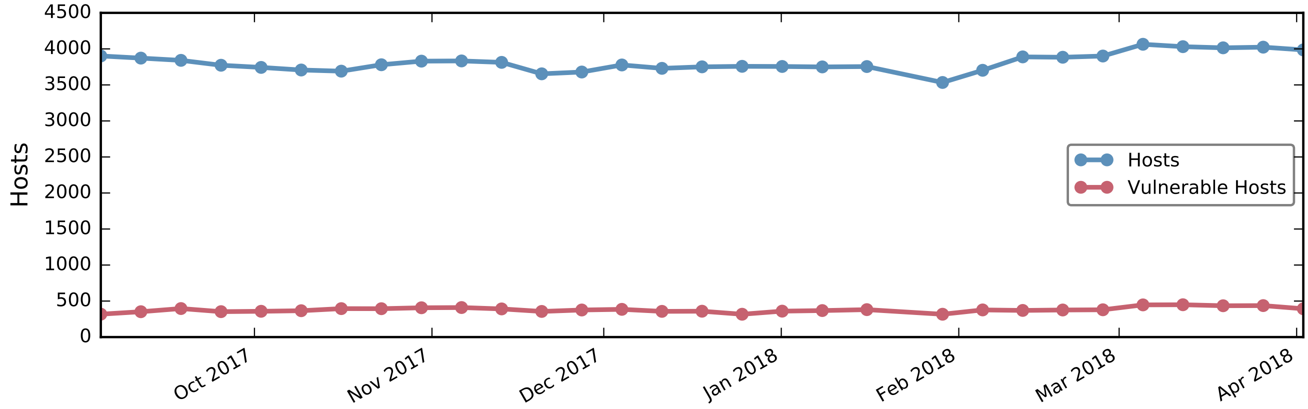


Figure 14: Vulnerable Hosts Over Time

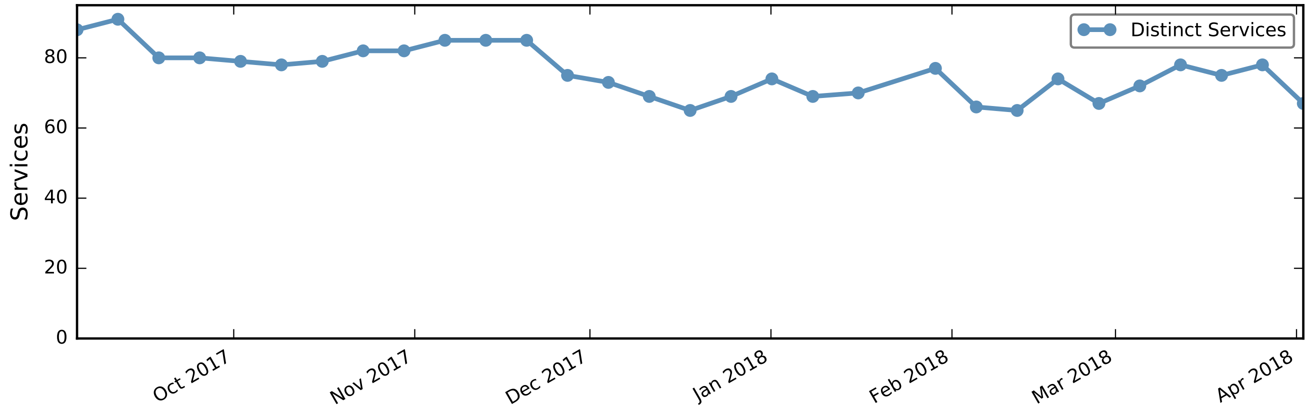


Figure 15: Distinct Services Over Time

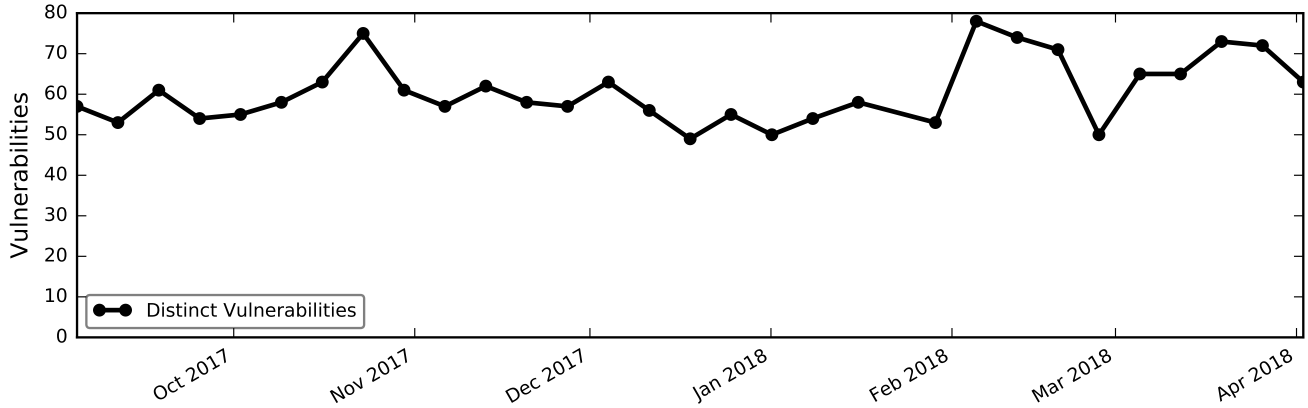


Figure 16: Distinct Vulnerabilities Over Time

	Previous Report	Current Report	% Change
Hosts	4,024	3,986	-1.0%
Vulnerable Hosts	437	393	-11.0%
Distinct Services	78	67	-15.0%
Distinct Vulnerabilities	72	63	-13.0%
Distinct Operating Systems	132	132	0.0%

Table 9: Comparison with Previous Report

Overall, for all hosts identified, SAMPLE averaged 0.29 vulnerabilities per host. For vulnerable hosts, SAMPLE averaged 2.95 total vulnerabilities per host. By severity, vulnerable hosts averaged 0.03 critical, 0.01 high, 2.66 medium, and 0.26 low vulnerabilities per host.

9 Conclusion

SAMPLE should use the data provided in this report to correct any identified vulnerabilities, configuration errors, and security concerns in your external network perimeter. If SAMPLE has questions, comments, or concerns about the findings or data contained in this report, please work with your designated technical point of contact when requesting assistance from NCATS at ncats@hq.dhs.gov.

Appendix A Vulnerability Summary

This section presents counts of all distinct vulnerabilities that were detected in the latest scans. It shows the name of the vulnerability, the severity level of the vulnerability, and the number of vulnerability detections in the previous report vs. this report. Low, medium, high, and critical vulnerabilities are displayed.

Vulnerability	Severity	Previous	Current	Change
MikroTik RouterOS < 6.41.3 SMB Buffer Overflow	Critical	4	4	0.0%
MikroTik RouterOS HTTP Server Arbitrary Write RCE (ChimayRed)	Critical	3	3	0.0%
Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE	Critical	4	3	-25.0%
OpenSSL Unsupported	Critical	1	0	-100.0%
FTP Privileged Port Bounce Scan	High	0	1	-%
PHP 5.6.x < 5.6.34 Stack Buffer Overflow	High	2	2	0.0%
SNMP Agent Default Community Name (public)	High	1	1	0.0%
Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities	High	1	0	-100.0%
Apache .htaccess and .htpasswd Disclosure	Medium	0	2	-%
Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	Medium	0	1	-%
Web Server Uses Non Random Session IDs	Medium	0	1	-%
Web Server Generic Cookie Injection	Medium	1	2	100.0%
DNS Server Cache Snooping Remote Information Disclosure	Medium	1	2	100.0%
DNS Server Recursive Query Cache Poisoning Weakness	Medium	1	2	100.0%
DNS Server Spoofed Request Amplification DDoS	Medium	1	2	100.0%
OpenSSL 1.1.0 < 1.1.0g RSA/DSA Unspecified Carry Issue	Medium	1	1	0.0%
TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)	Medium	2	2	0.0%
Terminal Services Doesn’t Use Network Level Authentication (NLA) Only	Medium	1	1	0.0%
Terminal Services Encryption Level is Medium or Low	Medium	1	1	0.0%
ASP.NET DEBUG Method Enabled	Medium	1	1	0.0%
Multiple Vendor Embedded FTP Service Any Username Authentication Bypass	Medium	1	1	0.0%
Network Time Protocol (NTP) Mode 6 Scanner	Medium	1	1	0.0%
PHP 5.6.x < 5.6.31 Multiple Vulnerabilities	Medium	2	2	0.0%
PHP 5.6.x < 5.6.32 Multiple Vulnerabilities	Medium	2	2	0.0%
PHP 5.6.x < 5.6.33 Multiple Vulnerabilities	Medium	2	2	0.0%
Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Medium	1	1	0.0%
SSL Certificate Expiry	Medium	69	65	-5.8%
SSL Certificate Signed Using Weak Hashing Algorithm	Medium	79	73	-7.6%
SSL Certificate Cannot Be Trusted	Medium	350	319	-8.9%
Return Of Bleichenbacher’s Oracle Threat (ROBOT) Information Disclosure	Medium	52	47	-9.6%
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	36	32	-11.1%
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Medium	9	8	-11.1%
SSL Self-Signed Certificate	Medium	203	180	-11.3%
SSL Medium Strength Cipher Suites Supported	Medium	131	114	-13.0%
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	73	61	-16.4%
Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)	Medium	6	5	-16.7%
HTTP TRACE / TRACK Methods Allowed	Medium	5	4	-20.0%
Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	Medium	15	12	-20.0%
SSL Version 2 and 3 Protocol Detection	Medium	14	11	-21.4%
SSL Weak Cipher Suites Supported	Medium	40	31	-22.5%
Unencrypted Telnet Server	Medium	16	12	-25.0%
SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	26	19	-26.9%
Web Application Potentially Vulnerable to Clickjacking	Medium	16	11	-31.2%
Web Server Generic XSS	Medium	6	4	-33.3%
Apache Tomcat Default Files	Medium	3	2	-33.3%

Vulnerability	Severity	Previous	Current	Change
Apache Server ETag Header Information Disclosure	Medium	2	1	-50.0%
OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Medium	2	1	-50.0%
SSH Weak Algorithms Supported	Medium	4	2	-50.0%
SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)	Medium	2	1	-50.0%
AXIS gSOAP Message Handling RCE (ACV-116267) (Devil's Ivy)	Medium	2	1	-50.0%
mDNS Detection (Remote Network)	Medium	3	1	-66.7%
Apache 2.4.x < 2.4.12 Multiple Vulnerabilities	Medium	1	0	-100.0%
Apache 2.4.x < 2.4.16 Multiple Vulnerabilities	Medium	1	0	-100.0%
OpenSSL 0.9.8 < 0.9.8zd Multiple Vulnerabilities (FREAK)	Medium	1	0	-100.0%
OpenSSL 0.9.8 < 0.9.8zf Multiple Vulnerabilities	Medium	1	0	-100.0%
Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)	Medium	1	0	-100.0%
Apache 2.4.x < 2.4.27 Multiple Vulnerabilities	Medium	1	0	-100.0%
Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed)	Medium	1	0	-100.0%
Microsoft Exchange Client Access Server Information Disclosure	Medium	1	0	-100.0%
OpenSSL 0.9.8 < 0.9.8zg Multiple Vulnerabilities	Medium	1	0	-100.0%
OpenSSL 0.9.8 < 0.9.8zh X509_ATTRIBUTE Memory Leak DoS	Medium	1	0	-100.0%
SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Medium	1	0	-100.0%
Web Server Load Balancer Detection	Low	0	1	-%
Anonymous FTP Enabled	Low	2	2	0.0%
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	Low	24	24	0.0%
POP3 Cleartext Logins Permitted	Low	1	1	0.0%
Terminal Services Encryption Level is not FIPS-140 Compliant	Low	1	1	0.0%
MikroTik RouterOS < 6.39.3 / 6.40.4 / 6.41rc (KRACK)	Low	1	1	0.0%
FTP Supports Cleartext Authentication	Low	4	3	-25.0%
Web Server Uses Basic Authentication Without HTTPS	Low	8	6	-25.0%
Web Server Transmits Cleartext Credentials	Low	55	38	-30.9%
SSH Server CBC Mode Ciphers Enabled	Low	18	11	-38.9%
SSH Weak MAC Algorithms Enabled	Low	15	9	-40.0%
OpenSSL AES-NI Padding Oracle MitM Information Disclosure	Low	2	1	-50.0%
Web Server HTTP Header Internal IP Disclosure	Low	4	2	-50.0%
Dropbear SSH Server < 2016.72 Multiple Vulnerabilities	Low	3	1	-66.7%
SSL Anonymous Cipher Suites Supported	Low	3	0	-100.0%

Appendix B Vulnerability Changes Since Last Report

B.1 Mitigated Vulnerabilities

This section lists the vulnerabilities that were included on the previous report, but were not detected by the latest scans. The table provides the initial detection and mitigation detection dates, plus the number of days it took to mitigate each vulnerability.

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Mitigation Detected (UTC)	Days To Mitigate
SUB_ORG	OpenSSL Unsupported	Critical	x.x.194.153	8100	2018-03-13	2018-04-03 14:37	21
SUB_ORG	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE	Critical	x.x.195.86	49152	2018-03-05	2018-03-28 06:17	23
SUB_ORG	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities	High	x.x.194.153	8100	2018-03-13	2018-04-03 14:37	21
SUB_ORG	AXIS gSOAP Message Handling RCE (ACV-116267) (Devil's Ivy)	Medium	x.x.147.214	NA	2018-03-13	NA	NA
SUB_ORG	Apache 2.4.x < 2.4.12 Multiple Vulnerabilities	Medium	x.x.194.153	8100	2018-03-13	2018-04-03 14:37	21
SUB_ORG	Apache 2.4.x < 2.4.16 Multiple Vulnerabilities	Medium	x.x.194.153	8100	2018-03-13	2018-04-03 14:37	21
SUB_ORG	Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)	Medium	x.x.194.153	8100	2018-03-13	2018-04-03 14:37	21
SUB_ORG	Apache 2.4.x < 2.4.27 Multiple Vulnerabilities	Medium	x.x.194.153	8100	2018-03-13	2018-04-03 14:37	21
SUB_ORG	Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed)	Medium	x.x.194.153	8100	2018-03-13	2018-04-03 14:37	21
SUB_ORG	Apache Server ETag Header Information Disclosure	Medium	x.x.80.153	443	2016-02-25	2018-03-31 03:54	765
SUB_ORG	Apache Tomcat Default Files	Medium	x.x.241.186	443	2018-02-02	NA	NA
SUB_ORG	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)	Medium	x.x.105.72	500	2017-02-02	NA	NA
SUB_ORG	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)	Medium	x.x.89.138	500	2017-02-02	NA	NA
SUB_ORG	HTTP TRACE / TRACK Methods Allowed	Medium	x.x.109.141	443	2017-08-30	NA	NA
SUB_ORG	HTTP TRACE / TRACK Methods Allowed	Medium	x.x.109.181	443	2017-08-30	2018-03-27 16:50	209
SUB_ORG	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	Medium	x.x.105.72	500	2012-11-27	NA	NA
SUB_ORG	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	Medium	x.x.80.229	500	2017-04-20	NA	NA
SUB_ORG	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	Medium	x.x.80.232	500	2012-11-27	NA	NA
SUB_ORG	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	Medium	x.x.80.237	500	2017-11-14	2018-03-27 05:44	133

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Mitigation Detected (UTC)	Days To Mitigate
SUB_ORG	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	Medium	x.x.83.162	500	2012-11-27	NA	NA
SUB_ORG	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	Medium	x.x.89.138	500	2014-07-26	NA	NA
SUB_ORG	Microsoft Exchange Client Access Server Information Disclosure	Medium	x.x.5.195	443	2017-01-06	2018-03-28 14:27	446
SUB_ORG	OpenSSL 0.9.8 < 0.9.8zd Multiple Vulnerabilities (FREAK)	Medium	x.x.194.153	8100	2018-03-13	2018-04-03 14:37	21
SUB_ORG	OpenSSL 0.9.8 < 0.9.8zf Multiple Vulnerabilities	Medium	x.x.194.153	8100	2018-03-13	2018-04-03 14:37	21
SUB_ORG	OpenSSL 0.9.8 < 0.9.8zg Multiple Vulnerabilities	Medium	x.x.194.153	8100	2018-03-13	2018-04-03 14:37	21
SUB_ORG	OpenSSL 0.9.8 < 0.9.8zh X509_ATTRIBUTE Memory Leak DoS	Medium	x.x.194.153	8100	2018-03-13	2018-04-03 14:37	21
SUB_ORG	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_ CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Medium	x.x.84.104	443	2016-11-30	NA	NA
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.77.138	443	2017-12-27	2018-04-01 02:32	95
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.77.140	443	2018-01-06	2018-03-29 04:54	82
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.80.10	443	2018-01-01	NA	NA
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.81.124	443	2018-01-01	2018-03-31 14:40	89
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.84.103	443	2018-01-04	2018-03-31 10:11	86
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.84.104	443	2017-12-30	2018-03-30 12:52	90
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.84.115	443	2017-12-29	NA	NA
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.84.117	443	2018-01-03	2018-03-27 11:57	83
SUB_ORG	SSH Weak Algorithms Supported	Medium	x.x.124.226	22	2017-08-30	2018-03-29 00:34	210
SUB_ORG	SSH Weak Algorithms Supported	Medium	x.x.192.34	22	2018-03-04	NA	NA
SUB_ORG	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Medium	x.x.124.236	443	2017-08-30	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.105.92	9443	2018-03-17	2018-03-29 22:05	12
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.109.121	9443	2018-03-04	2018-03-27 17:59	23
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.109.228	443	2017-08-30	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.124.226	21	2017-08-30	2018-04-02 02:11	214
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.124.226	443	2017-08-30	2018-04-02 02:11	214
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.151.98	443	2017-09-18	NA	NA

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Mitigation Detected (UTC)	Days To Mitigate
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.153.60	9443	2018-03-05	2018-04-01 17:35	28
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.158.35	443	2017-10-19	2018-04-02 02:40	165
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.158.37	443	2017-11-29	2018-04-01 04:40	123
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.163.121	9443	2018-03-11	2018-04-01 05:56	21
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.191.11	443	2017-04-25	2018-04-02 00:21	341
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.192.229	9443	2018-03-05	2018-03-31 20:04	26
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.193.151	9443	2018-03-05	2018-03-29 23:15	25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.194.154	9443	2018-03-05	2018-03-26 22:52	21
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.194.92	9443	2018-03-04	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.195.101	9443	2018-03-05	2018-03-31 10:51	26
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.195.115	9443	2018-03-04	2018-03-29 05:16	25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.195.146	9443	2018-03-05	2018-03-31 13:56	26
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.195.17	9443	2018-03-04	2018-03-29 06:06	25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.195.19	9443	2018-03-04	2018-03-29 04:57	25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.195.68	9443	2018-03-04	2018-03-29 08:28	25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.195.78	9443	2018-03-04	2018-03-29 22:06	25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.195.85	9443	2018-03-04	2018-03-29 04:48	25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.195.86	9443	2018-03-05	2018-03-28 06:17	23
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.196.166	9443	2018-03-04	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.196.45	9443	2018-03-04	2018-03-29 02:21	25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.208.143	443	2017-10-23	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.41.176	9443	2018-03-05	2018-04-01 04:57	27
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.41.185	9443	2018-03-04	2018-04-02 03:54	29
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.52.235	9443	2018-03-04	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.69.14	443	2016-04-15	2018-04-01 14:50	716
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.77.138	443	2017-08-30	2018-04-01 02:32	213
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.168	443	2016-09-03	2018-03-31 04:11	573
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.40	443	2017-05-01	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.81.67	443	2012-11-27	2018-03-31 13:57	1951
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.83.72	443	2018-01-13	2018-03-28 03:37	74
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.83.87	443	2017-09-15	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.83.93	443	2018-03-22	2018-03-26 09:35	4
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.84.117	443	2018-03-10	2018-03-27 11:57	17
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.156	443	2018-01-30	2018-03-29 03:01	57
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.194	443	2017-05-04	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.204	443	2018-03-25	2018-03-29 19:09	4
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.205	443	2017-04-19	2018-03-27 14:08	342
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.58	443	2016-09-10	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.70	443	2016-09-06	NA	NA

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Mitigation Detected (UTC)	Days To Mitigate
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.87.226	443	2016-07-20	2018-03-26 11:06	614
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.87.227	2010	2016-08-14	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.91.160	443	2016-07-19	2018-03-31 11:38	620
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.91.161	443	2017-02-15	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.91.173	443	2016-07-21	2018-03-31 09:22	618
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.91.195	443	2016-07-21	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.91.224	443	2017-01-22	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.92.39	443	2017-06-10	2018-03-31 13:57	294
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.92.93	443	2017-04-22	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.95.101	2010	2015-04-09	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.95.102	2010	2016-08-13	NA	NA
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.95.30	443	2016-04-24	2018-03-26 23:25	701
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.99.37	443	2015-10-20	2018-03-27 06:21	888
SUB_ORG	SSL Certificate Expiry	Medium	x.x.109.228	443	2017-08-30	NA	NA
SUB_ORG	SSL Certificate Expiry	Medium	x.x.80.15	443	2018-03-23	2018-03-31 13:02	8
SUB_ORG	SSL Certificate Expiry	Medium	x.x.85.70	443	2017-10-10	NA	NA
SUB_ORG	SSL Certificate Expiry	Medium	x.x.85.93	443	2017-10-09	NA	NA
SUB_ORG	SSL Certificate Expiry	Medium	x.x.87.227	2010	2016-08-14	NA	NA
SUB_ORG	SSL Certificate Expiry	Medium	x.x.95.101	2010	2016-08-13	NA	NA
SUB_ORG	SSL Certificate Expiry	Medium	x.x.95.102	2010	2016-08-13	NA	NA
SUB_ORG	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	x.x.124.226	21	2017-08-30	2018-04-02 02:11	214
SUB_ORG	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	x.x.124.226	443	2017-08-30	2018-04-02 02:11	214
SUB_ORG	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	x.x.151.98	443	2017-09-18	NA	NA
SUB_ORG	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	x.x.83.72	443	2018-03-24	2018-03-28 03:37	4
SUB_ORG	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	x.x.85.156	443	2018-01-30	2018-03-29 03:01	57
SUB_ORG	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	x.x.85.70	443	2018-01-16	NA	NA
SUB_ORG	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	x.x.91.195	443	2018-01-14	NA	NA
SUB_ORG	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	x.x.92.93	443	2018-01-13	NA	NA
SUB_ORG	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	x.x.95.1	443	2018-02-22	2018-03-27 17:19	33
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.141	443	2017-09-07	NA	NA
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.181	443	2017-08-30	2018-03-27 16:50	209
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.204	443	2017-11-28	NA	NA
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.219	443	2017-09-06	2018-04-01 13:01	207
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.220	443	2017-09-20	2018-04-01 22:59	193
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.221	443	2017-09-20	2018-03-31 18:34	192
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.222	443	2017-08-30	2018-03-31 21:27	213
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.124.226	21	2017-08-30	2018-04-02 02:11	214
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.124.226	443	2017-08-30	2018-04-02 02:11	214
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.158.10	443	2017-11-28	2018-04-01 22:11	124

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Mitigation Detected (UTC)	Days To Mitigate
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.158.35	443	2017-10-19	2018-04-02 02:40	165
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.158.37	443	2017-11-29	2018-04-01 04:40	123
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.255.143	443	2017-09-13	2018-03-28 14:49	196
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.59.83	25	2017-04-13	NA	NA
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.59.83	143	2017-04-13	NA	NA
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.59.83	465	2017-04-13	NA	NA
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.59.83	993	2017-04-13	NA	NA
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.80.157	443	2016-12-10	NA	NA
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.80.168	443	2016-12-09	2018-03-31 04:11	476
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.80.29	443	2016-12-11	NA	NA
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.80.40	443	2017-05-01	NA	NA
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.80.45	443	2017-05-16	NA	NA
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.81.118	443	2016-12-11	2018-03-31 02:54	474
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.81.67	443	2016-12-09	2018-03-31 13:57	477
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.83.87	443	2017-09-15	NA	NA
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.84.104	443	2016-12-08	NA	NA
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.85.121	443	2016-12-17	2018-03-31 04:11	468
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.85.58	443	2016-12-08	NA	NA
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.87.227	2010	2016-12-10	2018-03-26 20:14	472
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.88.181	443	2016-12-11	2018-03-31 04:14	475
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.88.182	443	2018-03-10	2018-03-31 10:21	21
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.90.196	443	2016-12-09	2018-03-27 03:51	472
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.90.202	443	2017-01-03	NA	NA
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.91.169	443	2016-12-09	NA	NA
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.91.224	443	2017-01-22	NA	NA
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.141	443	2017-09-07	NA	NA
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.181	443	2017-08-30	2018-03-27 16:50	209
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.204	443	2017-11-28	NA	NA
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.219	443	2017-09-06	2018-04-01 13:01	207
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.220	443	2017-09-20	2018-04-01 22:59	193
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.221	443	2017-09-20	2018-03-31 18:34	192
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.222	443	2017-08-30	2018-03-31 21:27	213
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.151.98	443	2017-09-18	NA	NA
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.158.10	443	2017-11-28	2018-04-01 22:11	124
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.59.83	25	2017-04-13	NA	NA
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.59.83	143	2017-04-13	NA	NA
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.59.83	465	2017-04-13	NA	NA
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.59.83	993	2017-04-13	NA	NA
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.80.21	443	2017-03-03	NA	NA

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Mitigation Detected (UTC)	Days To Mitigate
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.80.29	443	2016-07-19	NA	NA
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.83.87	443	2017-09-15	NA	NA
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.84.104	443	2016-11-30	NA	NA
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.85.121	443	2016-04-25	2018-03-31 04:11	704
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.87.227	2010	2015-08-27	2018-03-26 20:14	943
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.88.181	443	2016-01-13	2018-03-31 04:14	807
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.88.182	443	2018-03-10	2018-03-31 10:21	21
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.91.169	443	2016-08-19	NA	NA
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.91.224	443	2017-01-22	NA	NA
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.105.92	9443	2018-03-17	2018-03-29 22:05	12
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.109.121	9443	2018-03-04	2018-03-27 17:59	23
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.124.226	21	2017-08-30	2018-04-02 02:11	214
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.124.226	443	2017-08-30	2018-04-02 02:11	214
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.151.98	443	2017-09-18	NA	NA
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.153.60	9443	2018-03-05	2018-04-01 17:35	28
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.158.35	443	2017-10-19	2018-04-02 02:40	165
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.158.37	443	2017-11-29	2018-04-01 04:40	123
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.163.121	9443	2018-03-11	2018-04-01 05:56	21
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.192.229	9443	2018-03-05	2018-03-31 20:04	26
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.193.151	9443	2018-03-05	2018-03-29 23:15	25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.194.154	9443	2018-03-05	2018-03-26 22:52	21
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.194.92	9443	2018-03-04	NA	NA
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.195.101	9443	2018-03-05	2018-03-31 10:51	26
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.195.115	9443	2018-03-04	2018-03-29 05:16	25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.195.146	9443	2018-03-05	2018-03-31 13:56	26
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.195.17	9443	2018-03-04	2018-03-29 06:06	25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.195.19	9443	2018-03-04	2018-03-29 04:57	25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.195.68	9443	2018-03-04	2018-03-29 08:28	25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.195.78	9443	2018-03-04	2018-03-29 22:06	25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.195.85	9443	2018-03-04	2018-03-29 04:48	25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.195.86	9443	2018-03-05	2018-03-28 06:17	23
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.196.166	9443	2018-03-04	NA	NA
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.196.45	9443	2018-03-04	2018-03-29 02:21	25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.41.176	9443	2018-03-05	2018-04-01 04:57	27
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.41.185	9443	2018-03-04	2018-04-02 03:54	29
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.52.235	9443	2018-03-04	NA	NA
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.168	443	2017-09-22	2018-03-31 04:11	190
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.83.72	443	2018-03-24	2018-03-28 03:37	4
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.85.156	443	2018-01-30	2018-03-29 03:01	57

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Mitigation Detected (UTC)	Days To Mitigate
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.85.58	443	2016-09-10	NA	NA
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.85.70	443	2016-09-06	NA	NA
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.91.195	443	2016-07-21	NA	NA
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.92.93	443	2017-04-22	NA	NA
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.99.37	443	2015-10-20	2018-03-27 06:21	888
SUB_ORG	SSL Version 2 and 3 Protocol Detection	Medium	x.x.151.98	443	2017-09-18	NA	NA
SUB_ORG	SSL Version 2 and 3 Protocol Detection	Medium	x.x.80.157	443	2015-02-19	NA	NA
SUB_ORG	SSL Version 2 and 3 Protocol Detection	Medium	x.x.84.104	443	2016-11-30	NA	NA
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.141	443	2017-09-07	NA	NA
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.181	443	2017-08-30	2018-03-27 16:50	209
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.204	443	2017-11-28	NA	NA
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.219	443	2017-09-06	2018-04-01 13:01	207
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.220	443	2017-09-20	2018-04-01 22:59	193
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.221	443	2017-09-20	2018-03-31 18:34	192
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.222	443	2017-08-30	2018-03-31 21:27	213
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.80.29	443	2016-07-19	NA	NA
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.83.87	443	2017-09-15	NA	NA
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.84.104	443	2016-11-30	NA	NA
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.87.227	2010	2015-08-27	2018-03-26 20:14	943
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.88.181	443	2016-01-13	2018-03-31 04:14	807
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.88.182	443	2018-03-10	2018-03-31 10:21	21
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.91.169	443	2016-08-19	NA	NA
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.91.224	443	2017-04-25	2018-03-27 03:04	336
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.141	443	2017-09-07	NA	NA
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.142	443	2017-09-14	2018-04-01 19:52	199
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.143	443	2017-11-28	2018-03-28 09:49	120
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.151	443	2017-08-30	2018-03-27 13:33	209
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.181	443	2017-08-30	2018-03-27 16:50	209
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.204	443	2017-11-28	NA	NA
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.219	443	2017-09-06	2018-04-01 13:01	207
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.220	443	2017-09-20	2018-04-01 22:59	193
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.221	443	2017-09-20	2018-03-31 18:34	192
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.222	443	2017-08-30	2018-03-31 21:27	213
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.158.10	443	2017-11-28	2018-04-01 22:11	124
SUB_ORG	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)	Medium	x.x.84.104	443	2016-11-30	NA	NA
SUB_ORG	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	x.x.80.29	443	2016-07-19	NA	NA

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Mitigation Detected (UTC)	Days To Mitigate
SUB_ORG	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	x.x.83.87	443	2017-09-15	NA	NA
SUB_ORG	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	x.x.84.104	443	2016-11-30	NA	NA
SUB_ORG	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	x.x.87.227	2010	2015-08-27	2018-03-26 20:14	943
SUB_ORG	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	x.x.88.181	443	2016-01-13	2018-03-31 04:14	807
SUB_ORG	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	x.x.88.182	443	2018-03-10	2018-03-31 10:21	21
SUB_ORG	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	x.x.91.169	443	2016-08-19	NA	NA
SUB_ORG	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	x.x.91.224	443	2017-04-25	2018-03-27 03:04	336
SUB_ORG	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Medium	x.x.84.104	443	2016-11-30	NA	NA
SUB_ORG	Unencrypted Telnet Server	Medium	x.x.127.185	23	2018-03-25	2018-03-29 22:13	4
SUB_ORG	Unencrypted Telnet Server	Medium	x.x.136.93	2131	2018-03-23	2018-03-27 23:41	4
SUB_ORG	Unencrypted Telnet Server	Medium	x.x.163.121	2332	2018-03-11	2018-04-01 05:56	21
SUB_ORG	Unencrypted Telnet Server	Medium	x.x.195.57	2332	2018-03-05	2018-03-30 08:18	25
SUB_ORG	Unencrypted Telnet Server	Medium	x.x.195.86	2332	2018-03-05	2018-03-28 06:17	23
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.109.151	443	2017-09-16	2018-03-27 13:33	192
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.109.219	443	2017-09-14	2018-04-01 13:01	199
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.109.220	443	2017-09-20	2018-04-01 22:59	193
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.12.165	65000	2017-09-18	NA	NA
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.143.101	80	2017-09-20	2018-04-01 15:08	194
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.143.101	443	2017-10-17	2018-03-28 12:48	162
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.226.86	9191	2018-03-04	2018-03-28 04:12	23
SUB_ORG	Web Server Generic XSS	Medium	x.x.175.46	80	2018-01-13	2018-03-27 16:34	74
SUB_ORG	Web Server Generic XSS	Medium	x.x.175.46	7547	2018-01-13	2018-03-27 16:34	74
SUB_ORG	Web Server Generic XSS	Medium	x.x.81.118	9091	2017-10-01	2018-03-31 02:07	180
SUB_ORG	mDNS Detection (Remote Network)	Medium	x.x.195.121	5353	2018-03-04	2018-03-29 03:28	25
SUB_ORG	mDNS Detection (Remote Network)	Medium	x.x.195.124	5353	2018-03-04	2018-03-29 05:08	25
SUB_ORG	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities	Low	x.x.193.151	22	2018-03-05	2018-03-29 23:15	25
SUB_ORG	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities	Low	x.x.195.68	22	2018-03-04	2018-03-29 08:28	25
SUB_ORG	FTP Supports Cleartext Authentication	Low	x.x.195.86	21	2018-03-05	2018-03-28 06:17	23
SUB_ORG	OpenSSL AES-NI Padding Oracle MitM Information Disclosure	Low	x.x.124.226	21	2017-08-30	2018-04-02 02:11	214
SUB_ORG	SSH Server CBC Mode Ciphers Enabled	Low	x.x.105.72	22	2014-02-05	2018-03-30 04:43	1514
SUB_ORG	SSH Server CBC Mode Ciphers Enabled	Low	x.x.192.34	22	2018-03-04	NA	NA

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Mitigation Detected (UTC)	Days To Mitigate
SUB_ORG	SSH Server CBC Mode Ciphers Enabled	Low	x.x.193.151	22	2018-03-05	2018-03-29 23:15	25
SUB_ORG	SSH Server CBC Mode Ciphers Enabled	Low	x.x.195.68	22	2018-03-04	2018-03-29 08:28	25
SUB_ORG	SSH Server CBC Mode Ciphers Enabled	Low	x.x.81.118	33001	2016-02-28	NA	NA
SUB_ORG	SSH Server CBC Mode Ciphers Enabled	Low	x.x.89.178	22	2014-02-05	2018-04-02 00:28	1516
SUB_ORG	SSH Server CBC Mode Ciphers Enabled	Low	x.x.89.198	22	2014-02-05	2018-04-01 21:43	1517
SUB_ORG	SSH Weak MAC Algorithms Enabled	Low	x.x.105.72	22	2014-02-05	2018-03-30 04:43	1514
SUB_ORG	SSH Weak MAC Algorithms Enabled	Low	x.x.192.34	22	2018-03-04	NA	NA
SUB_ORG	SSH Weak MAC Algorithms Enabled	Low	x.x.193.151	22	2018-03-05	2018-03-29 23:15	25
SUB_ORG	SSH Weak MAC Algorithms Enabled	Low	x.x.195.68	22	2018-03-04	2018-03-29 08:28	25
SUB_ORG	SSH Weak MAC Algorithms Enabled	Low	x.x.89.178	22	2014-02-05	2018-04-02 00:28	1516
SUB_ORG	SSH Weak MAC Algorithms Enabled	Low	x.x.89.198	22	2014-02-05	2018-04-01 21:43	1517
SUB_ORG	SSL Anonymous Cipher Suites Supported	Low	x.x.124.226	21	2017-09-20	2018-04-02 02:11	194
SUB_ORG	SSL Anonymous Cipher Suites Supported	Low	x.x.59.83	25	2017-04-13	NA	NA
SUB_ORG	SSL Anonymous Cipher Suites Supported	Low	x.x.59.83	465	2017-04-13	NA	NA
SUB_ORG	Web Server HTTP Header Internal IP Disclosure	Low	x.x.109.151	443	2017-08-30	2018-03-31 15:46	213
SUB_ORG	Web Server HTTP Header Internal IP Disclosure	Low	x.x.194.153	8100	2018-03-13	2018-04-03 14:37	21
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.109.115	9191	2018-03-04	NA	NA
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.12.165	65000	2017-09-18	NA	NA
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.147.214	9191	2018-03-05	NA	NA
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.153.60	9191	2018-03-05	2018-04-01 17:35	28
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.163.121	9191	2018-03-11	2018-04-01 05:56	21
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.192.229	9191	2018-03-14	2018-03-31 20:04	18
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.192.24	9191	2018-03-08	2018-03-29 22:29	21
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.192.34	9191	2018-03-04	NA	NA
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.193.113	9191	2018-03-14	2018-03-27 06:52	12
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.193.151	9191	2018-03-05	2018-03-29 23:15	25
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.193.205	9191	2018-03-04	NA	NA
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.194.153	9191	2018-03-14	2018-04-03 14:37	20
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.194.233	9191	2018-03-05	NA	NA
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.195.101	9191	2018-03-14	2018-03-31 10:51	16
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.195.115	9191	2018-03-04	2018-03-29 05:16	25
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.195.19	9191	2018-03-08	2018-03-29 04:57	21
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.195.57	9191	2018-03-09	2018-03-30 08:18	21
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.195.69	9191	2018-03-04	2018-03-28 22:31	24
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.195.78	9191	2018-03-04	2018-03-29 22:06	25
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.195.85	9191	2018-03-04	2018-03-29 04:48	25
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.195.86	9191	2018-03-05	2018-03-28 06:17	23
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.196.13	9191	2018-03-13	2018-03-30 21:27	17
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.196.137	9191	2018-03-04	NA	NA

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Mitigation Detected (UTC)	Days To Mitigate
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.196.45	9191	2018-03-04	2018-03-29 02:21	25
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.226.86	9191	2018-03-04	2018-03-28 04:12	23
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.41.176	9191	2018-03-05	2018-04-01 04:57	27
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.41.185	9191	2018-03-04	2018-03-29 01:51	25
SUB_ORG	Web Server Uses Basic Authentication Without HTTPS	Low	x.x.105.92	8000	2018-03-04	2018-03-29 22:05	25
SUB_ORG	Web Server Uses Basic Authentication Without HTTPS	Low	x.x.195.19	8000	2018-03-04	2018-03-29 04:57	25
SUB_ORG	Web Server Uses Basic Authentication Without HTTPS	Low	x.x.41.166	8000	2018-03-05	2018-03-26 21:23	22
SUB_ORG	Web Server Uses Basic Authentication Without HTTPS	Low	x.x.81.118	9091	2017-09-15	2018-03-31 02:07	197

B.2 New Vulnerabilities Detected

This section lists the new vulnerabilities that were detected for the first time in the latest scans. The table provides the initial detection and latest detection dates for each vulnerabilty.

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)
SUB_ORG	Web Server Uses Non Random Session IDs	Medium	x.x.83.76	443	2018-03-29 08:06	2018-03-29 08:06
SUB_ORG	Web Server Uses Basic Authentication Without HTTPS	Low	x.x.194.196	8080	2018-03-29 07:40	2018-03-29 07:40

B.3 Re-Detected (Previously-Mitigated) Vulnerabilities

This section lists the vulnerabilities that were previously detected, then mitigated, and were re-detected in the latest scans. The table provides the initial detection and latest detection dates for each vulnerabilty.

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	Age Days
SUB_ORG	FTP Privileged Port Bounce Scan	High	x.x.124.236	21	2017-09-03 19:19	2018-04-04 08:21	212
SUB_ORG	Apache .htaccess and .htpasswd Disclosure	Medium	x.x.80.26	443	2018-01-29 23:31	2018-04-01 14:02	61
SUB_ORG	Apache .htaccess and .htpasswd Disclosure	Medium	x.x.80.27	443	2018-01-31 22:11	2018-04-03 06:46	61
SUB_ORG	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)	Medium	x.x.250.84	500	2017-02-03 03:50	2018-04-02 09:41	423
SUB_ORG	DNS Server Cache Snooping Remote Information Disclosure	Medium	x.x.192.34	53	2018-03-04 12:34	2018-04-04 07:20	30
SUB_ORG	DNS Server Recursive Query Cache Poisoning Weakness	Medium	x.x.192.34	53	2018-03-04 12:34	2018-04-04 07:20	30

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	Age Days
SUB_ORG	DNS Server Spoofed Request Amplification DDoS	Medium	x.x.192.34	53	2018-03-04 12:34	2018-04-04 07:20	30
SUB_ORG	HTTP TRACE / TRACK Methods Allowed	Medium	x.x.109.139	443	2018-02-08 10:17	2018-03-29 21:03	49
SUB_ORG	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	Medium	x.x.196.130	500	2016-04-27 02:55	2018-04-02 10:16	705
SUB_ORG	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	Medium	x.x.250.84	500	2013-03-12 04:09	2018-04-02 09:41	1847
SUB_ORG	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	Medium	x.x.80.231	500	2017-05-22 20:27	2018-04-04 12:13	316
SUB_ORG	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	Medium	x.x.192.34	53	2018-03-04 12:34	2018-04-03 16:14	30
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.81.123	443	2017-12-30 12:18	2018-03-31 11:57	90
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.84.114	443	2017-12-27 21:14	2018-04-03 12:59	96
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.85.80	443	2017-12-31 16:58	2018-03-31 17:08	90
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.109.115	9443	2018-03-04 17:22	2018-04-04 00:14	30
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.162.12	443	2017-08-30 18:55	2018-03-31 09:50	212
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.165.65	443	2017-11-28 21:21	2018-04-03 11:26	125
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.18.40	443	2018-03-02 11:00	2018-04-01 02:46	29
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.191.38	25	2017-03-13 02:51	2018-04-03 07:30	386
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.191.40	25	2017-03-11 09:46	2018-04-02 11:02	387
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.193.12	9443	2018-03-04 11:02	2018-04-02 11:22	29
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.193.149	9443	2018-03-04 15:11	2018-04-01 06:12	27
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.194.196	9443	2018-03-04 12:09	2018-04-02 10:16	28
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.195.245	9443	2018-03-04 23:16	2018-04-04 02:15	30
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.196.130	443	2016-04-27 02:55	2018-04-02 10:16	705
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.196.94	9443	2018-03-05 17:07	2018-03-31 15:34	25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.196.96	9443	2018-03-04 10:51	2018-04-04 11:50	31
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.208.141	443	2016-04-20 03:51	2018-04-01 17:00	711
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.241.232	443	2017-12-20 02:17	2018-04-01 05:53	102
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.79.162	25	2017-08-30 19:05	2018-04-03 04:50	215
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.16	443	2016-09-04 12:02	2018-04-03 11:27	575
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.177	443	2016-09-01 04:16	2018-03-31 18:00	576
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.58	443	2018-01-19 19:15	2018-04-01 12:12	71
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.81.150	443	2017-05-29 08:44	2018-04-03 18:26	309
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.84.114	443	2018-03-10 01:00	2018-04-03 12:59	24
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.165	443	2017-11-19 01:20	2018-04-01 19:36	133
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.55	443	2016-09-02 14:24	2018-04-03 15:53	578

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	Age Days
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.95	443	2016-09-06 05:50	2018-04-03 16:03	574
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.87.20	443	2018-01-26 13:16	2018-03-30 13:30	63
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.88.224	443	2017-02-04 06:44	2018-04-01 12:36	421
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.91.200	443	2016-11-12 22:58	2018-04-01 05:04	504
SUB_ORG	SSL Certificate Expiry	Medium	x.x.241.232	443	2017-12-20 02:17	2018-04-01 05:53	102
SUB_ORG	SSL Certificate Expiry	Medium	x.x.85.95	443	2017-10-10 14:16	2018-04-03 16:03	175
SUB_ORG	SSL Certificate Expiry	Medium	x.x.91.200	443	2017-08-27 20:16	2018-04-01 05:04	216
SUB_ORG	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	x.x.79.162	25	2017-08-30 19:05	2018-04-03 04:50	215
SUB_ORG	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	x.x.85.95	443	2018-01-13 17:26	2018-04-03 16:03	79
SUB_ORG	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	x.x.91.249	443	2017-05-13 08:21	2018-03-31 18:29	322
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.100.234	443	2016-12-13 05:10	2018-04-01 16:19	474
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.131	443	2017-09-20 21:54	2018-04-01 08:27	192
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.139	443	2018-02-12 13:18	2018-04-02 22:09	49
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.201	443	2017-09-06 19:08	2018-04-04 11:40	209
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.203	443	2017-09-20 22:49	2018-04-02 14:43	193
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.209	443	2017-09-13 21:54	2018-04-01 12:54	199
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.217	443	2017-09-13 21:15	2018-03-29 01:44	196
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.224	443	2017-09-06 19:06	2018-04-02 09:43	207
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.162.12	443	2017-08-30 18:55	2018-03-31 09:50	212
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.165.65	443	2017-12-02 23:15	2018-04-03 11:26	121
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.80.12	443	2018-02-13 07:21	2018-04-03 12:35	49
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.80.16	443	2016-12-10 12:15	2018-04-03 11:27	478
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.80.177	443	2016-12-13 08:11	2018-03-31 18:00	473
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.85.112	443	2016-12-08 21:01	2018-04-01 02:04	478
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.85.204	443	2017-11-22 11:52	2018-04-02 21:50	131
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.85.55	443	2016-12-18 14:47	2018-04-03 15:53	471
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.88.224	443	2017-02-04 06:44	2018-04-01 12:36	421
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.91.249	443	2017-05-13 08:21	2018-03-31 18:29	322
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.139	443	2018-02-12 13:18	2018-04-02 22:09	49
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.201	443	2017-09-06 19:08	2018-04-04 11:40	209
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.203	443	2017-09-20 22:49	2018-04-02 14:43	193
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.209	443	2017-09-13 21:54	2018-04-01 12:54	199
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.217	443	2017-09-13 21:15	2018-03-29 01:44	196
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.224	443	2017-09-06 19:06	2018-04-02 09:43	207
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.165.65	443	2017-12-02 23:15	2018-04-03 11:26	121
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.80.177	443	2015-07-16 14:15	2018-03-31 18:00	989
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.85.204	443	2017-11-22 11:52	2018-04-02 21:50	131
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.88.224	443	2017-02-04 06:44	2018-04-01 12:36	421
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.91.249	443	2017-05-13 08:21	2018-03-31 18:29	322

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Latest Detection	Age
					(UTC)	(UTC)	Days
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.109.115	9443	2018-03-04 17:22	2018-04-04 00:14	30
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.193.12	9443	2018-03-04 11:02	2018-04-02 11:22	29
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.193.149	9443	2018-03-04 15:11	2018-04-01 06:12	27
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.194.196	9443	2018-03-04 12:09	2018-04-02 10:16	28
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.195.245	9443	2018-03-04 23:16	2018-04-04 02:15	30
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.196.130	443	2016-04-27 02:55	2018-04-02 10:16	705
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.196.94	9443	2018-03-05 17:07	2018-03-31 15:34	25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.196.96	9443	2018-03-04 10:51	2018-04-04 11:50	31
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.79.162	25	2017-08-30 19:05	2018-04-03 04:50	215
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.58	443	2018-02-02 22:10	2018-04-01 12:12	57
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.85.55	443	2016-09-02 14:24	2018-04-03 15:53	578
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.85.95	443	2016-09-06 05:50	2018-04-03 16:03	574
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.139	443	2018-02-12 13:18	2018-04-02 22:09	49
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.201	443	2017-09-06 19:08	2018-04-04 11:40	209
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.203	443	2017-09-20 22:49	2018-04-02 14:43	193
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.217	443	2017-09-13 21:15	2018-03-29 01:44	196
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.224	443	2017-09-06 19:06	2018-04-02 09:43	207
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.91.249	443	2017-05-13 08:21	2018-03-31 18:29	322
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.139	443	2018-02-12 13:18	2018-04-02 22:09	49
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.201	443	2017-09-06 19:08	2018-04-04 11:40	209
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.203	443	2017-09-20 22:49	2018-04-02 14:43	193
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.217	443	2017-09-13 21:15	2018-03-29 01:44	196
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.224	443	2017-09-06 19:06	2018-04-02 09:43	207
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.45.66	443	2017-09-27 23:43	2018-04-03 20:23	187
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.85.112	443	2016-07-18 15:44	2018-04-01 02:04	621
SUB_ORG	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	x.x.91.249	443	2017-05-13 08:21	2018-03-31 18:29	322
SUB_ORG	Unencrypted Telnet Server	Medium	x.x.250.84	6002	2017-06-08 01:00	2018-04-02 09:41	298
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.109.217	443	2017-09-17 22:41	2018-03-29 01:44	192
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.81.126	443	2017-09-16 13:21	2018-03-30 22:48	195
SUB_ORG	Web Server Generic Cookie Injection	Medium	x.x.87.205	80	2017-03-05 16:01	2018-04-01 12:39	391
SUB_ORG	Web Server Generic XSS	Medium	x.x.87.205	80	2017-09-15 19:49	2018-04-01 12:39	197
SUB_ORG	Web Server Load Balancer Detection	Low	x.x.93.146	443	2015-04-08 08:54	2018-03-31 13:17	1088
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.192.16	9191	2018-03-14 23:28	2018-04-01 08:38	17
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.193.12	9191	2018-03-04 11:02	2018-04-02 11:22	29
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.193.149	9191	2018-03-04 15:11	2018-04-01 06:12	27
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.194.150	9191	2018-03-05 14:26	2018-04-03 00:17	28
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.196.134	9191	2018-03-04 17:51	2018-04-02 12:34	28
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.196.200	9191	2018-03-05 03:31	2018-04-02 15:13	28

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	Age Days
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.196.250	9191	2018-03-05 12:17	2018-04-04 10:41	29
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.196.94	9191	2018-03-05 17:07	2018-03-31 15:34	25
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.197.47	9191	2018-03-04 20:48	2018-04-04 13:35	30
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.9.184	9191	2018-03-04 14:46	2018-03-30 10:47	25
SUB_ORG	Web Server Uses Basic Authentication Without HTTPS	Low	x.x.195.142	8080	2018-03-09 02:53	2018-04-03 00:51	24

B.4 Recently-Detected Vulnerabilities

This section lists the vulnerabilities that were detected since the last report, but not detected in the latest scans. The table provides the initial detection and latest detection dates for each vulnerabilty. It is **strongly recommended** to verify if the vulnerabilities below were actively mitigated by your organization. If they were not, it is highly likely these vulnerabilities will be detected again by future scans.

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	Age Days
SUB_ORG	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE	Critical	x.x.195.86	49152	2018-03-05 18:15	2018-03-27 16:08	21
SUB_ORG	OpenSSL Unsupported	Critical	x.x.194.153	8100	2018-03-13 12:30	2018-04-03 01:30	20
SUB_ORG	Linux FTP Server Backdoor Detection	Critical	x.x.124.236	21	2018-03-31 02:24	2018-03-31 02:24	0
SUB_ORG	Default Password for FTP 'admin' Account	Critical	x.x.124.236	21	2018-03-31 02:24	2018-03-31 02:24	0
SUB_ORG	WFTP Unpassworded Guest Account	Critical	x.x.124.236	21	2018-03-31 02:24	2018-03-31 02:24	0
SUB_ORG	Windows FTP Server NULL Administrator Password	Critical	x.x.124.236	21	2018-03-31 02:24	2018-03-31 02:24	0
SUB_ORG	XAMPP Default FTP Account	High	x.x.124.236	21	2017-09-18 15:45	2018-03-31 02:24	193
SUB_ORG	Small SSH RSA Key	High	x.x.105.72	22	2018-01-28 04:02	2018-04-01 00:20	62
SUB_ORG	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities	High	x.x.194.153	8100	2018-03-13 12:30	2018-04-03 01:30	20
SUB_ORG	Emerson SM-Ethernet FTP Server Default Credentials	High	x.x.124.236	21	2018-03-31 02:24	2018-03-31 02:24	0
SUB_ORG	Janitza Hard-Coded FTP Password	High	x.x.124.236	21	2018-03-31 02:24	2018-03-31 02:24	0
SUB_ORG	Wyse Device Manager Default FTP Account	High	x.x.124.236	21	2018-03-31 02:24	2018-03-31 02:24	0
SUB_ORG	PFTP Default Unpassworded Account	High	x.x.124.236	21	2018-03-31 02:24	2018-03-31 02:24	0
SUB_ORG	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	Medium	x.x.83.163	500	2012-11-26 22:43	2018-03-31 03:55	1950
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.81.67	443	2012-11-27 01:41	2018-03-27 11:42	1946
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.90.211	443	2015-07-06 00:11	2018-03-31 02:39	999
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.90.211	443	2015-07-06 00:11	2018-03-31 02:39	999
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.80.153	443	2015-10-10 22:55	2018-03-31 03:21	902
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.90.183	8443	2016-01-03 16:34	2018-03-29 04:55	815
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.88.181	443	2016-01-13 22:23	2018-03-27 02:15	803

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	Age Days
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.88.181	443	2016-01-13 22:23	2018-03-27 02:15	803
SUB_ORG	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	x.x.88.181	443	2016-01-13 22:23	2018-03-27 02:15	803
SUB_ORG	Apache Server ETag Header Information Disclosure	Medium	x.x.80.153	443	2016-02-25 13:44	2018-03-26 23:59	760
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.69.14	443	2016-04-15 11:28	2018-03-28 12:48	712
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.85.121	443	2016-04-25 22:27	2018-03-27 00:43	700
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.91.160	443	2016-07-19 22:26	2018-03-27 07:20	615
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.91.173	443	2016-07-21 18:50	2018-03-27 01:48	613
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.82.146	443	2016-07-29 20:55	2018-03-31 01:41	609
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.90.183	8443	2016-09-01 03:36	2018-03-29 04:55	574
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.90.183	8443	2016-09-01 03:36	2018-03-29 04:55	574
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.168	443	2016-09-03 21:11	2018-03-27 00:47	569
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.84.103	443	2016-09-06 10:57	2018-03-31 09:53	570
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.83.35	443	2016-12-09 10:02	2018-03-31 03:50	476
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.81.67	443	2016-12-09 13:01	2018-03-27 11:42	472
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.80.153	443	2016-12-09 13:49	2018-03-31 03:21	476
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.80.168	443	2016-12-09 21:36	2018-03-27 00:47	472
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.90.211	443	2016-12-09 23:38	2018-03-31 02:39	476
SUB_ORG	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	x.x.84.103	443	2016-12-10 06:17	2018-03-31 09:53	476
SUB_ORG	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)	Medium	x.x.84.103	443	2016-12-10 06:17	2018-03-31 09:53	476
SUB_ORG	SSL Version 2 and 3 Protocol Detection	Medium	x.x.84.103	443	2016-12-10 06:17	2018-03-31 09:53	476
SUB_ORG	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Medium	x.x.84.103	443	2016-12-10 06:17	2018-03-31 09:53	476
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.84.103	443	2016-12-10 06:17	2018-03-31 09:53	476
SUB_ORG	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Medium	x.x.84.103	443	2016-12-10 06:17	2018-03-31 09:53	476
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.84.103	443	2016-12-10 06:17	2018-03-31 09:53	476
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.84.103	443	2016-12-10 06:17	2018-03-31 09:53	476
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.82.146	443	2016-12-10 16:10	2018-03-31 01:41	475
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.88.181	443	2016-12-11 10:30	2018-03-27 02:15	470
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.81.118	443	2016-12-11 18:43	2018-03-27 00:53	470
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.85.121	443	2016-12-17 20:55	2018-03-27 00:43	464
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.90.183	8443	2017-01-01 18:28	2018-03-29 04:55	451
SUB_ORG	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	x.x.88.188	443	2017-02-11 21:46	2018-03-30 13:07	411
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.88.188	443	2017-02-11 21:46	2018-03-30 13:07	411

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	Age Days
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.88.188	443	2017-02-11 21:46	2018-03-30 13:07	411
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.88.188	443	2017-02-11 21:46	2018-03-30 13:07	411
SUB_ORG	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	Medium	x.x.80.235	500	2017-04-21 21:57	2018-03-30 12:46	342
SUB_ORG	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	x.x.91.175	443	2017-04-24 17:12	2018-03-31 03:52	340
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.91.175	443	2017-04-24 17:12	2018-03-31 03:52	340
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.91.175	443	2017-04-24 17:12	2018-03-31 03:52	340
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.91.175	443	2017-04-24 17:12	2018-03-31 03:52	340
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.191.11	443	2017-04-25 17:09	2018-03-28 20:21	337
SUB_ORG	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	x.x.91.156	443	2017-05-06 11:59	2018-03-31 03:58	328
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.91.156	443	2017-05-06 11:59	2018-03-31 03:58	328
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.91.156	443	2017-05-06 11:59	2018-03-31 03:58	328
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.91.156	443	2017-05-06 11:59	2018-03-31 03:58	328
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.82.192	443	2017-06-04 22:13	2018-03-27 14:52	295
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.52	443	2017-06-08 20:10	2018-03-31 09:59	295
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.52	443	2017-06-08 20:10	2018-03-31 09:59	295
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.92.39	443	2017-06-10 19:39	2018-03-27 11:05	289
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.233	443	2017-07-31 01:36	2018-03-30 11:08	242
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.233	443	2017-07-31 01:36	2018-03-30 11:08	242
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.80.233	443	2017-07-31 01:36	2018-03-30 11:08	242
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.80.51	443	2017-07-31 02:01	2018-03-31 01:34	242
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.80.51	443	2017-07-31 02:01	2018-03-31 01:34	242
SUB_ORG	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	x.x.95.1	443	2017-08-22 13:14	2018-03-27 17:14	217
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.95.1	443	2017-08-22 13:14	2018-03-27 17:14	217
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.95.1	443	2017-08-22 13:14	2018-03-27 17:14	217
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.95.1	443	2017-08-22 13:14	2018-03-27 17:14	217
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.82.194	443	2017-08-25 00:16	2018-03-31 03:32	218
SUB_ORG	SSL Certificate Expiry	Medium	x.x.82.194	443	2017-08-25 00:16	2018-03-31 03:32	218
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.88.187	443	2017-08-27 04:02	2018-03-30 11:50	215
SUB_ORG	SSL Certificate Expiry	Medium	x.x.88.187	443	2017-08-27 04:02	2018-03-30 11:50	215
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.124.226	21	2017-08-30 17:28	2018-03-29 00:24	210
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.124.226	443	2017-08-30 17:28	2018-03-29 00:24	210
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.124.226	21	2017-08-30 17:28	2018-03-29 00:24	210
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.124.226	443	2017-08-30 17:28	2018-03-29 00:24	210
SUB_ORG	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	x.x.124.226	21	2017-08-30 17:28	2018-03-29 00:24	210
SUB_ORG	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	x.x.124.226	443	2017-08-30 17:28	2018-03-29 00:24	210

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Latest Detection	Age
					(UTC)	(UTC)	Days
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.124.226	21	2017-08-30 17:28	2018-03-29 00:24	210
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.124.226	443	2017-08-30 17:28	2018-03-29 00:24	210
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.222	443	2017-08-30 17:29	2018-03-27 19:44	209
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.222	443	2017-08-30 17:29	2018-03-27 19:44	209
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.222	443	2017-08-30 17:29	2018-03-27 19:44	209
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.222	443	2017-08-30 17:29	2018-03-27 19:44	209
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.136.75	443	2017-08-30 18:32	2018-03-30 23:14	212
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.77.138	443	2017-08-30 18:41	2018-03-28 01:39	209
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.162.12	443	2017-08-30 18:55	2018-03-31 09:50	212
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.162.12	443	2017-08-30 18:55	2018-03-31 09:50	212
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.219	443	2017-09-06 18:54	2018-03-28 09:33	202
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.219	443	2017-09-06 18:54	2018-03-28 09:33	202
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.219	443	2017-09-06 18:54	2018-03-28 09:33	202
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.219	443	2017-09-06 18:54	2018-03-28 09:33	202
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.223	8443	2017-09-06 18:54	2018-03-27 00:23	201
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.82.192	443	2017-09-07 05:05	2018-03-27 14:52	201
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.217	443	2017-09-13 21:15	2018-03-29 01:44	196
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.217	443	2017-09-13 21:15	2018-03-29 01:44	196
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.217	443	2017-09-13 21:15	2018-03-29 01:44	196
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.217	443	2017-09-13 21:15	2018-03-29 01:44	196
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.109.219	443	2017-09-14 22:35	2018-03-28 09:33	194
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.142	443	2017-09-14 22:43	2018-03-28 17:15	194
SUB_ORG	IIS Detailed Error Information Disclosure	Medium	x.x.255.149	443	2017-09-16 00:56	2018-03-26 11:06	191
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.81.126	443	2017-09-16 13:21	2018-03-30 22:48	195
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.109.217	443	2017-09-17 22:41	2018-03-29 01:44	192
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.109.222	443	2017-09-17 23:14	2018-03-27 19:44	190
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.143.101	80	2017-09-20 02:43	2018-03-28 13:15	189
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.109.220	443	2017-09-20 20:40	2018-03-28 20:09	188
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.220	443	2017-09-20 20:40	2018-03-28 20:09	188
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.220	443	2017-09-20 20:40	2018-03-28 20:09	188
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.220	443	2017-09-20 20:40	2018-03-28 20:09	188
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.220	443	2017-09-20 20:40	2018-03-28 20:09	188
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.109.221	443	2017-09-20 22:07	2018-03-27 16:31	187
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.221	443	2017-09-20 22:07	2018-03-27 16:31	187
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.221	443	2017-09-20 22:07	2018-03-27 16:31	187
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.109.221	443	2017-09-20 22:07	2018-03-27 16:31	187
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.168	443	2017-09-22 03:44	2018-03-27 00:47	185
SUB_ORG	Backup Files Disclosure	Medium	x.x.80.107	80	2017-09-22 15:01	2018-03-26 10:22	184
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.80.107	80	2017-09-22 15:01	2018-03-26 10:22	184

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	Age Days
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.109.207	443	2017-09-27 23:45	2018-03-31 00:09	184
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.109.207	443	2017-09-27 23:45	2018-03-31 00:09	184
SUB_ORG	Web Server Generic XSS	Medium	x.x.81.118	9091	2017-10-01 18:22	2018-03-27 00:53	176
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.158.35	443	2017-10-19 04:57	2018-03-28 10:30	160
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.158.35	443	2017-10-19 04:57	2018-03-28 10:30	160
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.158.35	443	2017-10-19 04:57	2018-03-28 10:30	160
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.90.62	443	2017-11-01 05:31	2018-03-30 11:37	149
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.81.241	443	2017-11-10 10:42	2018-03-31 02:16	140
SUB_ORG	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	x.x.158.10	443	2017-11-28 21:32	2018-03-28 18:33	119
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.158.10	443	2017-11-28 21:32	2018-03-28 18:33	119
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.158.10	443	2017-11-28 21:32	2018-03-28 18:33	119
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.158.10	443	2017-11-28 21:32	2018-03-28 18:33	119
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.158.10	443	2017-11-28 21:32	2018-03-28 18:33	119
SUB_ORG	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	x.x.158.10	443	2017-11-28 21:32	2018-03-28 18:33	119
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.158.37	443	2017-11-29 01:53	2018-03-28 02:10	119
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.158.37	443	2017-11-29 01:53	2018-03-28 02:10	119
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.158.37	443	2017-11-29 01:53	2018-03-28 02:10	119
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.77.138	443	2017-12-27 05:52	2018-03-28 01:39	90
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.80.52	443	2017-12-27 16:17	2018-03-31 09:59	93
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.90.211	443	2017-12-27 18:48	2018-03-31 02:39	93
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.84.104	443	2017-12-30 15:28	2018-03-26 10:04	85
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.83.35	443	2018-01-01 10:02	2018-03-31 03:50	88
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.81.124	443	2018-01-01 23:16	2018-03-27 12:07	84
SUB_ORG	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure	Medium	x.x.84.103	443	2018-01-04 12:23	2018-03-27 03:31	81
SUB_ORG	Web Server Generic XSS	Medium	x.x.175.46	7547	2018-01-13 01:23	2018-03-26 14:12	72
SUB_ORG	Web Server Generic XSS	Medium	x.x.175.46	80	2018-01-13 01:23	2018-03-26 14:12	72
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.83.86	443	2018-01-24 22:41	2018-03-28 10:52	62
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.87.20	443	2018-01-26 13:16	2018-03-30 13:30	63
SUB_ORG	HTTP TRACE / TRACK Methods Allowed	Medium	x.x.109.139	443	2018-02-08 10:17	2018-03-29 21:03	49
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.194.79	9443	2018-03-04 11:06	2018-03-29 08:34	24
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.194.79	9443	2018-03-04 11:06	2018-03-29 08:34	24
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.196.93	9443	2018-03-04 11:59	2018-03-29 05:01	24

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	Age Days
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.196.93	9443	2018-03-04 11:59	2018-03-29 05:01	24
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.41.185	9443	2018-03-04 12:16	2018-03-29 01:47	24
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.41.185	9443	2018-03-04 12:16	2018-03-29 01:47	24
SUB_ORG	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	Medium	x.x.192.34	53	2018-03-04 12:34	2018-04-03 16:14	30
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.9.184	9443	2018-03-04 14:46	2018-03-26 09:07	21
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.9.184	9443	2018-03-04 14:46	2018-03-26 09:07	21
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.108.29	9443	2018-03-04 17:09	2018-03-26 08:02	21
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.108.29	9443	2018-03-04 17:09	2018-03-26 08:02	21
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.192.24	9443	2018-03-04 19:06	2018-03-29 22:29	25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.192.24	9443	2018-03-04 19:06	2018-03-29 22:29	25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.195.142	9443	2018-03-04 19:28	2018-03-29 21:32	25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.195.142	9443	2018-03-04 19:28	2018-03-29 21:32	25
SUB_ORG	AXIS gSOAP Message Handling RCE (ACV-116267) (Devil's Ivy)	Medium	x.x.194.150	NA	2018-03-04 20:45	2018-04-03 14:16	29
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.194.150	9443	2018-03-04 20:45	2018-04-03 14:16	29
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.194.150	9443	2018-03-04 20:45	2018-04-03 14:16	29
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.105.90	9443	2018-03-05 00:07	2018-04-01 03:51	27
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.105.90	9443	2018-03-05 00:07	2018-04-01 03:51	27
SUB_ORG	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Medium	x.x.108.25	3389	2018-03-05 00:10	2018-03-30 00:33	25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.108.25	3389	2018-03-05 00:10	2018-03-30 00:33	25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.108.25	3389	2018-03-05 00:10	2018-03-30 00:33	25
SUB_ORG	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	x.x.108.25	3389	2018-03-05 00:10	2018-03-30 00:33	25
SUB_ORG	Terminal Services Encryption Level is Medium or Low	Medium	x.x.108.25	3389	2018-03-05 00:10	2018-03-30 00:33	25
SUB_ORG	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Medium	x.x.108.25	3389	2018-03-05 00:10	2018-03-30 00:33	25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.194.233	9443	2018-03-05 00:23	2018-03-30 01:21	25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.194.233	9443	2018-03-05 00:23	2018-03-30 01:21	25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.153.60	9443	2018-03-05 01:17	2018-03-28 15:59	23
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.153.60	9443	2018-03-05 01:17	2018-03-28 15:59	23
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.41.176	9443	2018-03-05 11:04	2018-03-28 01:21	22
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.41.176	9443	2018-03-05 11:04	2018-03-28 01:21	22
SUB_ORG	Unencrypted Telnet Server	Medium	x.x.195.57	2332	2018-03-05 11:50	2018-03-26 05:07	20
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.195.101	9443	2018-03-05 16:28	2018-03-27 08:57	21
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.195.101	9443	2018-03-05 16:28	2018-03-27 08:57	21
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.195.146	9443	2018-03-05 17:24	2018-03-27 07:39	21
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.195.146	9443	2018-03-05 17:24	2018-03-27 07:39	21
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.195.86	9443	2018-03-05 18:15	2018-03-27 16:08	21

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	Age Days
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.195.86	9443	2018-03-05 18:15	2018-03-27 16:08	21
SUB_ORG	Unencrypted Telnet Server	Medium	x.x.195.86	2332	2018-03-05 18:15	2018-03-27 16:08	21
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.192.229	9443	2018-03-05 18:33	2018-03-27 18:01	21
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.192.229	9443	2018-03-05 18:33	2018-03-27 18:01	21
SUB_ORG	Web Server Generic XSS	Medium	x.x.196.117	8080	2018-03-05 19:10	2018-03-30 18:21	24
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.157.83	9443	2018-03-05 19:54	2018-04-03 19:40	28
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.157.83	9443	2018-03-05 19:54	2018-04-03 19:40	28
SUB_ORG	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	x.x.88.182	443	2018-03-10 17:32	2018-03-27 02:03	16
SUB_ORG	SSL Medium Strength Cipher Suites Supported	Medium	x.x.88.182	443	2018-03-10 17:32	2018-03-27 02:03	16
SUB_ORG	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	x.x.88.182	443	2018-03-10 17:32	2018-03-27 02:03	16
SUB_ORG	SSL Weak Cipher Suites Supported	Medium	x.x.88.182	443	2018-03-10 17:32	2018-03-27 02:03	16
SUB_ORG	Unencrypted Telnet Server	Medium	x.x.163.121	2332	2018-03-11 17:01	2018-03-28 04:08	16
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.163.121	9443	2018-03-11 17:01	2018-03-28 04:08	16
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.163.121	9443	2018-03-11 17:01	2018-03-28 04:08	16
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.87.21	443	2018-03-12 15:11	2018-03-29 23:07	17
SUB_ORG	OpenSSL 0.9.8 < 0.9.8zd Multiple Vulnerabilities (FREAK)	Medium	x.x.194.153	8100	2018-03-13 12:30	2018-04-03 01:30	20
SUB_ORG	OpenSSL 0.9.8 < 0.9.8zf Multiple Vulnerabilities	Medium	x.x.194.153	8100	2018-03-13 12:30	2018-04-03 01:30	20
SUB_ORG	OpenSSL 0.9.8 < 0.9.8zh X509_ATTRIBUTE Memory Leak DoS	Medium	x.x.194.153	8100	2018-03-13 12:30	2018-04-03 01:30	20
SUB_ORG	OpenSSL 0.9.8 < 0.9.8zg Multiple Vulnerabilities	Medium	x.x.194.153	8100	2018-03-13 12:30	2018-04-03 01:30	20
SUB_ORG	Apache 2.4.x < 2.4.16 Multiple Vulnerabilities	Medium	x.x.194.153	8100	2018-03-13 12:30	2018-04-03 01:30	20
SUB_ORG	Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed)	Medium	x.x.194.153	8100	2018-03-13 12:30	2018-04-03 01:30	20
SUB_ORG	Apache 2.4.x < 2.4.27 Multiple Vulnerabilities	Medium	x.x.194.153	8100	2018-03-13 12:30	2018-04-03 01:30	20
SUB_ORG	Apache 2.4.x < 2.4.12 Multiple Vulnerabilities	Medium	x.x.194.153	8100	2018-03-13 12:30	2018-04-03 01:30	20
SUB_ORG	Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)	Medium	x.x.194.153	8100	2018-03-13 12:30	2018-04-03 01:30	20
SUB_ORG	Unencrypted Telnet Server	Medium	x.x.194.153	2332	2018-03-13 12:30	2018-04-03 01:30	20
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.194.153	9443	2018-03-13 12:30	2018-04-03 01:30	20
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.194.153	9443	2018-03-13 12:30	2018-04-03 01:30	20
SUB_ORG	SSL Certificate Expiry	Medium	x.x.80.15	443	2018-03-23 02:47	2018-03-27 04:26	4
SUB_ORG	Web Server Uses Non Random Session IDs	Medium	x.x.83.76	443	2018-03-29 08:06	2018-03-29 08:06	0
SUB_ORG	Default FTP Credentials (ntpupdate / ntpupdate)	Medium	x.x.124.236	21	2018-03-31 02:24	2018-03-31 02:24	0
SUB_ORG	Apache 2.4.x < 2.4.30 Multiple Vulnerabilities	Medium	x.x.194.153	8100	2018-04-01 03:34	2018-04-03 01:30	1
SUB_ORG	SSH Weak MAC Algorithms Enabled	Low	x.x.89.198	22	2014-02-05 01:04	2018-03-26 20:30	1510
SUB_ORG	SSH Server CBC Mode Ciphers Enabled	Low	x.x.89.198	22	2014-02-05 01:04	2018-03-26 20:30	1510
SUB_ORG	SSH Weak MAC Algorithms Enabled	Low	x.x.105.72	22	2014-02-05 06:50	2018-03-29 03:21	1512
SUB_ORG	SSH Server CBC Mode Ciphers Enabled	Low	x.x.105.72	22	2014-02-05 06:50	2018-03-29 03:21	1512
SUB_ORG	SSH Weak MAC Algorithms Enabled	Low	x.x.89.178	22	2014-02-05 14:20	2018-03-26 22:34	1510
SUB_ORG	SSH Server CBC Mode Ciphers Enabled	Low	x.x.89.178	22	2014-02-05 14:20	2018-03-26 22:34	1510
SUB_ORG	OpenSSL AES-NI Padding Oracle MitM Information Disclosure	Low	x.x.124.226	21	2017-08-30 17:28	2018-03-29 00:24	210

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	Age Days
SUB_ORG	Web Server HTTP Header Internal IP Disclosure	Low	x.x.109.151	443	2017-08-30 17:31	2018-03-27 13:23	208
SUB_ORG	Web Server PROPFIND Method Internal IP Disclosure	Low	x.x.255.149	443	2017-08-30 17:32	2018-03-26 11:06	207
SUB_ORG	Web Server Uses Basic Authentication Without HTTPS	Low	x.x.81.118	9091	2017-09-15 11:14	2018-03-27 00:53	192
SUB_ORG	SSL Anonymous Cipher Suites Supported	Low	x.x.124.226	21	2017-09-20 00:42	2018-03-29 00:24	189
SUB_ORG	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	Low	x.x.158.10	443	2017-11-28 21:32	2018-03-28 18:33	119
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.196.96	9191	2018-03-04 10:51	2018-04-03 20:38	30
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.194.79	9191	2018-03-04 11:06	2018-03-29 08:34	24
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.196.93	9191	2018-03-04 11:59	2018-03-29 05:01	24
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.194.196	9191	2018-03-04 12:09	2018-03-29 07:40	24
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.41.180	9191	2018-03-04 13:05	2018-03-30 06:03	25
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.41.168	9191	2018-03-04 14:44	2018-03-29 20:00	25
SUB_ORG	Terminal Services Encryption Level is not FIPS-140 Compliant	Low	x.x.108.25	3389	2018-03-05 00:10	2018-03-30 00:33	25
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.153.60	9191	2018-03-05 01:17	2018-03-28 15:59	23
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.196.200	9191	2018-03-05 03:31	2018-04-02 15:13	28
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.41.176	9191	2018-03-05 11:04	2018-03-28 01:21	22
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.194.154	9191	2018-03-05 11:33	2018-03-26 22:52	21
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.194.150	9191	2018-03-05 14:26	2018-04-03 00:17	28
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.195.86	9191	2018-03-05 18:15	2018-03-27 16:08	21
SUB_ORG	FTP Supports Cleartext Authentication	Low	x.x.195.86	21	2018-03-05 18:15	2018-03-27 16:08	21
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.192.133	9191	2018-03-09 01:42	2018-03-30 02:47	21
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.195.208	9191	2018-03-09 01:56	2018-03-30 02:28	21
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.195.57	9191	2018-03-09 15:48	2018-03-26 05:07	16
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.163.121	9191	2018-03-11 17:01	2018-03-28 04:08	16
SUB_ORG	Web Server HTTP Header Internal IP Disclosure	Low	x.x.194.153	8100	2018-03-13 12:30	2018-04-03 01:30	20
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.192.229	9191	2018-03-14 05:49	2018-03-27 18:01	13
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.194.153	9191	2018-03-14 17:15	2018-04-03 01:30	19
SUB_ORG	Web Server Uses Basic Authentication Without HTTPS	Low	x.x.195.101	8100	2018-03-14 23:45	2018-03-27 08:57	12
SUB_ORG	Web Server Transmits Cleartext Credentials	Low	x.x.195.101	9191	2018-03-14 23:45	2018-03-27 08:57	12
SUB_ORG	SSH Server CBC Mode Ciphers Enabled	Low	x.x.127.185	22	2018-03-25 20:27	2018-03-29 22:19	4
SUB_ORG	Web Server Uses Basic Authentication Without HTTPS	Low	x.x.163.121	8080	2018-03-28 04:08	2018-03-28 04:08	0
SUB_ORG	Web Server Uses Basic Authentication Without HTTPS	Low	x.x.194.196	8080	2018-03-29 07:40	2018-03-29 07:40	0

Appendix C Detailed Findings and Recommended Mitigations by Vulnerability

This section presents detailed scan results from the network mapping and vulnerability scans. Vulnerabilities identified have a recommended mitigation solution that should be considered in order to establish or maintain a secure network.

Vulnerability	Severity	CVSS	Solution
MikroTik RouterOS < 6.41.3 SMB Buffer Overflow	Critical	10.0	Upgrade to MikroTik RouterOS 6.41.3 or later.
	4 Affected Host(s): x.x.105.90, x.x.157.83, x.x.192.34, x.x.236.156 *Initial Detection:* 2018-03-23 00:26 UTC *Latest Detection:* 2018-04-04 11:56 UTC *Description:* According to its self-reported version, the remote networking device is running a version of MikroTik RouterOS before 6.41.3. It is, therefore, affected by a remote SMB buffer overflow vulnerability that can be leveraged by an unauthenticated, remote attacker to execute arbitrary code.		
MikroTik RouterOS HTTP Server Arbitrary Write RCE (ChimayRed)	Critical	10.0	Upgrade to MikroTik RouterOS version 6.38.5 or later.
	3 Affected Host(s): x.x.105.90, x.x.157.83, x.x.192.34 *Initial Detection:* 2018-03-04 12:34 UTC *Latest Detection:* 2018-04-04 09:30 UTC *Description:* The MikroTik RouterOS software running on the remote host is affected by a flaw in its HTTP web server process due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this, via a specially crafted POST request, to write data to an arbitrary location within the web server process, resulting in a denial of service condition or the execution of arbitrary code. Note that this vulnerability is reportedly part of the ChimayRed exploit from the Vault 7 leaks.		

Vulnerability	Severity	CVSS	Solution
Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE	Critical	10.0	Upgrade to libupnp version 1.6.18 or later. If libupnp is used as a third party library by a different application, contact the vendor of that application for a fix.
	3 Affected Host(s): x.x.194.150, x.x.196.200, x.x.196.96 *Initial Detection:* 2018-03-04 10:38 UTC *Latest Detection:* 2018-04-04 11:50 UTC *Description:* According to its banner, the version of Portable SDK for UPnP Devices (libupnp) running on the remote host is prior to 1.6.18. It is, therefore, affected by multiple remote code execution vulnerabilities : - A stack-based buffer overflow condition exists in the unique_service_name() function within file ssdp/ssdp_server.c when handling Simple Service Discovery Protocol (SSDP) requests that is triggered while copying the DeviceType URN. An unauthenticated, remote attacker can exploit this, via a specially crafted SSDP request, to execute arbitrary code. (CVE-2012-5958) - A stack-based buffer overflow condition exists in the unique_service_name() function within file ssdp/ssdp_server.c when handling Simple Service Discovery Protocol (SSDP) requests that is triggered while copying the UDN prior to two colons. An unauthenticated, remote attacker can exploit this, via a specially crafted SSDP request, to execute arbitrary code. (CVE-2012-5959) - A stack-based buffer overflow condition exists in the unique_service_name() function within file ssdp/ssdp_server.c when handling Simple Service Discovery Protocol (SSDP) requests that is triggered while copying the UDN prior to the '::upnp:rootdevice' string. An unauthenticated, remote attacker can exploit this, via a specially crafted SSDP request, to execute arbitrary code. (CVE-2012-5960) - Multiple stack-based buffer overflow conditions exist in the unique_service_name() function within file ssdp/ssdp_server.c due to improper validation of the UDN, DeviceType, and ServiceType fields when parsing Simple Service Discovery Protocol (SSDP) requests. An unauthenticated, remote attacker can exploit these issues, via a specially crafted SSDP request, to execute arbitrary code. (CVE-2012-5961, CVE-2012-5962, CVE-2012-5963, CVE-2012-5964, CVE-2012-5965)		
FTP Privileged Port Bounce Scan	High	7.5	See the CERT advisory in the references for solutions and workarounds.
	1 Affected Host(s): x.x.124.236 *Initial Detection:* 2017-09-03 19:19 UTC *Latest Detection:* 2018-04-04 08:21 UTC *Description:* It is possible to force the remote FTP server to connect to third parties using the PORT command. The problem allows intruders to use your network resources to scan other hosts, making them think the attack comes from your network.		

Vulnerability	Severity	CVSS	Solution
PHP 5.6.x < 5.6.34 Stack Buffer Overflow	High	7.5	Upgrade to PHP version 5.6.34 or later.
	1 Affected Host(s): x.x.124.231 *Initial Detection:* 2018-03-10 02:31 UTC *Latest Detection:* 2018-04-04 06:16 UTC *Description:* According to its banner, the version of PHP running on the remote web server is 5.6.x prior to 5.6.34. It is, therefore, affected by a stack buffer overflow vulnerability.		
SNMP Agent Default Community Name (public)	High	7.5	Disable the SNMP service on the remote host if you do not use it. Either filter incoming UDP packets going to this port, or change the default community string.
	1 Affected Host(s): x.x.175.46 *Initial Detection:* 2018-01-06 15:25 UTC *Latest Detection:* 2018-04-04 05:45 UTC *Description:* It is possible to obtain the default community name of the remote SNMP server. An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).		
AXIS gSOAP Message Handling RCE (ACV-116267) (Devil's Ivy)	Medium	6.8	Upgrade to the latest available firmware version for your device per the vendor advisory (ACV-116267).
	1 Affected Host(s): x.x.194.150 *Initial Detection:* 2018-03-04 20:45 UTC *Latest Detection:* 2018-04-03 14:16 UTC *Description:* The remote AXIS device is running a firmware version that is missing a security patch. It is, therefore, affected by a remote code execution vulnerability, known as Devil's Ivy, due to an overflow condition that exists in a third party SOAP library (gSOAP). An unauthenticated, remote attacker can exploit this, via an HTTP POST message exceeding 2GB of data, to trigger a stack-based buffer overflow, resulting in a denial of service condition or the execution of arbitrary code. An attacker who successfully exploits this vulnerability can reset the device to its factory defaults, change network settings, take complete control of the device, or reboot it to prevent an operator from viewing the feed.		
Apache Tomcat Default Files	Medium	6.8	Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.
	2 Affected Host(s): x.x.242.236, x.x.80.39 *Initial Detection:* 2018-01-28 03:16 UTC *Latest Detection:* 2018-04-03 23:57 UTC *Description:* The default error page, default index page, example JSPs, and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.		

Vulnerability	Severity	CVSS	Solution
Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Medium	6.4	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the ’Allow connections only from computers running Remote Desktop with Network Level Authentication’ setting if it is available.

1 Affected Host(s): x.x.108.25
Initial Detection: 2018-03-05 00:10 UTC
Latest Detection: 2018-03-30 00:33 UTC
Description: The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

Vulnerability	Severity	CVSS	Solution
SSL Certificate Cannot Be Trusted	Medium	6.4	Purchase or generate a proper certificate for this service.

309 Affected Host(s): x.x.10.2, x.x.101.3, x.x.108.25, x.x.109.115, x.x.109.150, x.x.109.229, x.x.109.230, x.x.12.165, x.x.121.222, x.x.124.231, x.x.124.236, x.x.136.74, x.x.136.75, x.x.136.76, x.x.136.81, x.x.136.82, x.x.15.174, x.x.151.66, x.x.157.83, x.x.158.11, x.x.162.12, x.x.165.38, x.x.165.39, x.x.165.65, x.x.166.126, x.x.18.40, x.x.184.100, x.x.184.204, x.x.184.99, x.x.191.10, x.x.191.38, x.x.191.40, x.x.192.133, x.x.192.16, x.x.192.20, x.x.192.24, x.x.192.34, x.x.193.109, x.x.193.113, x.x.193.12, x.x.193.130, x.x.193.138, x.x.193.149, x.x.193.205, x.x.193.95, x.x.194.150, x.x.194.153, x.x.194.170, x.x.194.188, x.x.194.196, x.x.194.207, x.x.194.233, x.x.194.79, x.x.195.142, x.x.195.145, x.x.195.146, x.x.195.199, x.x.195.208, x.x.195.245, x.x.196.10, x.x.196.117, x.x.196.119, x.x.196.130, x.x.196.134, x.x.196.137, x.x.196.194, x.x.196.200, x.x.196.253, x.x.196.93, x.x.196.94, x.x.196.96, x.x.197.23, x.x.197.35, x.x.197.47, x.x.208.130, x.x.208.141, x.x.208.142, x.x.208.47, x.x.212.145, x.x.228.130, x.x.241.232, x.x.27.11, x.x.27.34, x.x.41.161, x.x.41.166, x.x.41.168, x.x.41.180, x.x.5.195, x.x.59.83, x.x.62.142, x.x.79.162, x.x.80.107, x.x.80.12, x.x.80.122, x.x.80.137, x.x.80.140, x.x.80.15, x.x.80.150, x.x.80.157, x.x.80.158, x.x.80.159, x.x.80.16, x.x.80.162, x.x.80.166, x.x.80.167, x.x.80.170, x.x.80.172, x.x.80.177, x.x.80.186, x.x.80.23, x.x.80.232, x.x.80.233, x.x.80.24, x.x.80.26, x.x.80.27, x.x.80.33, x.x.80.39, x.x.80.41, x.x.80.51, x.x.80.52, x.x.80.54, x.x.80.56, x.x.80.57, x.x.80.58, x.x.81.138, x.x.81.150, x.x.81.187, x.x.81.241, x.x.82.147, x.x.82.194, x.x.82.195, x.x.82.196, x.x.82.197, x.x.82.199, x.x.82.201, x.x.82.202, x.x.82.203, x.x.82.204, x.x.83.140, x.x.83.162, x.x.83.163, x.x.83.35, x.x.83.36, x.x.83.88, x.x.83.89, x.x.84.103, x.x.84.104, x.x.84.113, x.x.84.114, x.x.84.115, x.x.84.116, x.x.84.118, x.x.84.119, x.x.84.120, x.x.84.145, x.x.84.2, x.x.84.3, x.x.84.38, x.x.84.4, x.x.84.81, x.x.84.82, x.x.84.88, x.x.84.90, x.x.84.91, x.x.84.92, x.x.84.93, x.x.85.106, x.x.85.107, x.x.85.112, x.x.85.122, x.x.85.123, x.x.85.132, x.x.85.139, x.x.85.140, x.x.85.141, x.x.85.142, x.x.85.145, x.x.85.146, x.x.85.155, x.x.85.159, x.x.85.160, x.x.85.162, x.x.85.163, x.x.85.165, x.x.85.168, x.x.85.169, x.x.85.176, x.x.85.180, x.x.85.183, x.x.85.191, x.x.85.199, x.x.85.30, x.x.85.32, x.x.85.5, x.x.85.55, x.x.85.56, x.x.85.57, x.x.85.59, x.x.85.60, x.x.85.61, x.x.85.72, x.x.85.75, x.x.85.76, x.x.85.78, x.x.85.79, x.x.85.85, x.x.85.86, x.x.85.87, x.x.85.88, x.x.85.89, x.x.85.9, x.x.85.90, x.x.85.91, x.x.85.93, x.x.85.94, x.x.85.95, x.x.87.145, x.x.87.17, x.x.87.20, x.x.87.21, x.x.87.227, x.x.87.228, x.x.87.26, x.x.87.3, x.x.87.4, x.x.87.61, x.x.88.138, x.x.88.177, x.x.88.178, x.x.88.179, x.x.88.180, x.x.88.181, x.x.88.182, x.x.88.183, x.x.88.185, x.x.88.186, x.x.88.187, x.x.88.188, x.x.88.189, x.x.88.224, x.x.89.148, x.x.89.152, x.x.89.153, x.x.89.40, x.x.89.41, x.x.90.182, x.x.90.183, x.x.90.201, x.x.90.202, x.x.90.207, x.x.90.211, x.x.90.62, x.x.90.74, x.x.91.147, x.x.91.156, x.x.91.159, x.x.91.162, x.x.91.163, x.x.91.164, x.x.91.165, x.x.91.167, x.x.91.168, x.x.91.169, x.x.91.175, x.x.91.192, x.x.91.193, x.x.91.194, x.x.91.196, x.x.91.197, x.x.91.200, x.x.91.201, x.x.91.202, x.x.91.208, x.x.91.211, x.x.91.212, x.x.91.235, x.x.91.236, x.x.91.249, x.x.91.254, x.x.92.10, x.x.92.132, x.x.92.47, x.x.92.7, x.x.92.80, x.x.92.81, x.x.92.82, x.x.92.83, x.x.92.84, x.x.92.85, x.x.92.86, x.x.92.87, x.x.92.88, x.x.92.9, x.x.92.90, x.x.92.91, x.x.92.92, x.x.92.94, x.x.93.146, x.x.93.147, x.x.93.148, x.x.94.35, x.x.95.1, x.x.95.100, x.x.95.101, x.x.95.102, x.x.95.108, x.x.95.26, x.x.95.29, x.x.95.32

Initial Detection: 2012-11-26 22:09 UTC

Latest Detection: 2018-04-04 13:35 UTC

Description: The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- 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 could not be verified. 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.

<table>
<tr><th>Vulnerability</th><th>Severity</th><th>CVSS</th><th>Solution</th></tr>
<tr><td>SSL Self-Signed Certificate</td><td>Medium</td><td>6.4</td><td>Purchase or generate a proper certificate for this service.</td></tr>
<tr><td></td><td colspan="3"><i>179 Affected Host(s):</i> x.x.10.2, x.x.101.3, x.x.108.25, x.x.109.115, x.x.109.150, x.x.12.165, x.x.121.222, x.x.124.231, x.x.124.236, x.x.157.83, x.x.158.11, x.x.165.38, x.x.165.39, x.x.166.126, x.x.192.133, x.x.192.16, x.x.192.20, x.x.192.24, x.x.192.34, x.x.193.109, x.x.193.113, x.x.193.12, x.x.193.130, x.x.193.138, x.x.193.149, x.x.193.205, x.x.193.95, x.x.194.150, x.x.194.153, x.x.194.170, x.x.194.188, x.x.194.196, x.x.194.207, x.x.194.233, x.x.194.79, x.x.195.142, x.x.195.145, x.x.195.146, x.x.195.199, x.x.195.208, x.x.195.245, x.x.196.10, x.x.196.117, x.x.196.119, x.x.196.130, x.x.196.134, x.x.196.137, x.x.196.194, x.x.196.200, x.x.196.253, x.x.196.93, x.x.196.94, x.x.196.96, x.x.197.23, x.x.197.35, x.x.197.47, x.x.208.130, x.x.228.130, x.x.27.11, x.x.27.34, x.x.41.161, x.x.41.166, x.x.41.168, x.x.41.180, x.x.79.162, x.x.80.12, x.x.80.122, x.x.80.137, x.x.80.140, x.x.80.150, x.x.80.157, x.x.80.158, x.x.80.159, x.x.80.172, x.x.80.186, x.x.80.23, x.x.80.232, x.x.80.233, x.x.80.26, x.x.80.27, x.x.80.52, x.x.80.54, x.x.80.58, x.x.81.241, x.x.83.35, x.x.83.36, x.x.84.145, x.x.84.88, x.x.84.90, x.x.84.91, x.x.84.92, x.x.84.93, x.x.85.123, x.x.85.132, x.x.85.139, x.x.85.140, x.x.85.141, x.x.85.142, x.x.85.155, x.x.85.159, x.x.85.162, x.x.85.163, x.x.85.30, x.x.85.32, x.x.85.5, x.x.85.55, x.x.85.56, x.x.85.57, x.x.85.59, x.x.85.60, x.x.85.61, x.x.85.72, x.x.85.75, x.x.85.76, x.x.85.78, x.x.85.79, x.x.85.85, x.x.85.86, x.x.85.87, x.x.85.88, x.x.85.89, x.x.85.9, x.x.85.90, x.x.85.91, x.x.85.93, x.x.85.94, x.x.85.95, x.x.87.26, x.x.87.3, x.x.87.4, x.x.87.61, x.x.88.138, x.x.89.148, x.x.89.152, x.x.89.153, x.x.89.41, x.x.90.183, x.x.90.201, x.x.90.202, x.x.90.207, x.x.90.211, x.x.90.74, x.x.91.147, x.x.91.156, x.x.91.159, x.x.91.162, x.x.91.163, x.x.91.164, x.x.91.165, x.x.91.167, x.x.91.168, x.x.91.169, x.x.91.175, x.x.91.192, x.x.91.193, x.x.91.194, x.x.91.196, x.x.91.197, x.x.91.249, x.x.91.254, x.x.92.80, x.x.92.81, x.x.92.82, x.x.92.83, x.x.92.84, x.x.92.85, x.x.92.86, x.x.92.87, x.x.92.88, x.x.92.90, x.x.92.91, x.x.92.92, x.x.92.94, x.x.93.146, x.x.93.147, x.x.93.148, x.x.95.1, x.x.95.100, x.x.95.32
<i>Initial Detection:</i> 2012-11-27 17:12 UTC
<i>Latest Detection:</i> 2018-04-04 13:35 UTC
<i>Description:</i> 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.</td></tr>
<tr><td>Web Server Uses Non Random Session IDs</td><td>Medium</td><td>6.4</td><td>Configure the remote site and CGIs so as to use random session IDs.</td></tr>
<tr><td></td><td colspan="3"><i>1 Affected Host(s):</i> x.x.83.76
<i>Initial Detection:</i> 2018-03-29 08:06 UTC
<i>Latest Detection:</i> 2018-03-29 08:06 UTC
<i>Description:</i> The remote web server generates a session ID for each connection. A session ID is typically used to keep track of the actions of a user while he visits a website.

The remote server generates non-random session IDs. An attacker might use this flaw to guess the session IDs of other users and therefore steal their session.</td></tr>
</table>

Vulnerability	Severity	CVSS	Solution
Unencrypted Telnet Server	Medium	5.8	Disable the Telnet service and use SSH instead.
	11 Affected Host(s): x.x.174.177, x.x.175.46, x.x.193.113, x.x.193.95, x.x.194.153, x.x.195.199, x.x.250.84, x.x.34.69, x.x.41.161, x.x.41.176, x.x.59.81 *Initial Detection:* 2013-03-12 04:09 UTC *Latest Detection:* 2018-04-04 05:45 UTC *Description:* The remote host is running a Telnet server over an unencrypted channel. Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server. SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.		
ASP.NET DEBUG Method Enabled	Medium	5.0	Make sure that DEBUG statements are disabled or only usable by authenticated users.
	1 Affected Host(s): x.x.255.159 *Initial Detection:* 2017-09-20 21:55 UTC *Latest Detection:* 2018-04-03 13:36 UTC *Description:* It is possible to send debug statements to the remote ASP scripts. An attacker might use this to alter the runtime of the remote scripts.		
Apache .htaccess and .htpasswd Disclosure	Medium	5.0	Change the Apache configuration to block access to these files.
	2 Affected Host(s): x.x.80.26, x.x.80.27 *Initial Detection:* 2018-01-29 23:31 UTC *Latest Detection:* 2018-04-03 06:46 UTC *Description:* The Apache server does not properly restrict access to .htaccess and/or .htpasswd files. A remote unauthenticated attacker can download these files and potentially uncover important information.		

Vulnerability	Severity	CVSS	Solution
Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)	Medium	5.0	Upgrade to the relevant fixed version referenced in Cisco bug ID CSCvb29204.
	5 Affected Host(s): x.x.250.84, x.x.80.235, x.x.80.236, x.x.80.237, x.x.89.137 *Initial Detection:* 2017-02-03 03:50 UTC *Latest Detection:* 2018-04-03 14:51 UTC *Description:* The IKE service running on the remote Cisco IOS device is affected by an information disclosure vulnerability, known as BENIGNCERTAIN, in the Internet Key Exchange version 1 (IKEv1) subsystem due to improper handling of IKEv1 security negotiation requests. An unauthenticated, remote attacker can exploit this issue, via a specially crafted IKEv1 packet, to disclose memory contents, resulting in the disclosure of confidential information including credentials and configuration settings. BENIGNCERTAIN is one of multiple Equation Group vulnerabilities and exploits disclosed on 2016/08/14 by a group known as the Shadow Brokers.		
DNS Server Cache Snooping Remote Information Disclosure	Medium	5.0	Contact the vendor of the DNS software for a fix.
	2 Affected Host(s): x.x.192.34, x.x.59.81 *Initial Detection:* 2017-03-06 19:26 UTC *Latest Detection:* 2018-04-04 07:20 UTC *Description:* The remote DNS server responds to queries for third-party domains that do not have the recursion bit set. This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited. For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more. Note: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.		

Vulnerability	Severity	CVSS	Solution
DNS Server Recursive Query Cache Poisoning Weakness	Medium	5.0	Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it). If you are using bind 8, you can do this by using the instruction ’allow-recursion’ in the ’options’ section of your named.conf. If you are using bind 9, you can define a grouping of internal addresses using the ’acl’ command. Then, within the options block, you can explicitly state: ’allow-recursion { hosts_defined_in_acl }’ If you are using another name server, consult its documentation.

2 Affected Host(s): x.x.192.34, x.x.59.81
Initial Detection: 2017-03-06 19:26 UTC
Latest Detection: 2018-04-04 07:20 UTC
Description: It is possible to query the remote name server for third-party names.

If this is your internal nameserver, then the attack vector may be limited to employees or guest access if allowed.

If you are probing a remote nameserver, then it allows anyone to use it to resolve third party names (such as www.nessus.org).
This allows attackers to perform cache poisoning attacks against this nameserver.

If the host allows these recursive queries via UDP, then the host can be used to ’bounce’ Denial of Service attacks against another network or system.

DNS Server Spoofed Request Amplification DDoS	Medium	5.0	Restrict access to your DNS server from public network or reconfigure it to reject such queries.

2 Affected Host(s): x.x.192.34, x.x.59.81
Initial Detection: 2017-03-06 19:26 UTC
Latest Detection: 2018-04-04 07:20 UTC
Description: The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone (’.’) and get an answer that is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this ’amplification’ to launch a denial of service attack against a third-party host using the remote DNS server.

Vulnerability	Severity	CVSS	Solution
Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	Medium	5.0	- Disable Aggressive Mode if supported. - Do not use Pre-Shared key for authentication if it's possible. - If using Pre-Shared key cannot be avoided, use very strong keys. - If possible, do not allow VPN connections from any IP addresses. Note that this plugin does not run over IPv6.
	12 Affected Host(s): x.x.196.130, x.x.228.130, x.x.250.84, x.x.80.230, x.x.80.231, x.x.80.235, x.x.81.72, x.x.83.163, x.x.87.3, x.x.89.137, x.x.92.10, x.x.92.9 *Initial Detection:* 2012-11-26 22:43 UTC *Latest Detection:* 2018-04-04 12:13 UTC *Description:* The remote Internet Key Exchange (IKE) version 1 service seems to support Aggressive Mode with Pre-Shared key (PSK) authentication. Such a configuration could allow an attacker to capture and crack the PSK of a VPN gateway and gain unauthorized access to private networks.		
Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	Medium	5.0	Contact your DNS server vendor for a patch.
	1 Affected Host(s): x.x.192.34 *Initial Detection:* 2018-03-04 12:34 UTC *Latest Detection:* 2018-04-03 16:14 UTC *Description:* The remote DNS resolver does not use random ports when making queries to third-party DNS servers. An unauthenticated, remote attacker can exploit this to poison the remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites.		
Multiple Vendor Embedded FTP Service Any Username Authentication Bypass	Medium	5.0	Correct the FTP server's configuration so that the service handles authentication requests properly.
	1 Affected Host(s): x.x.124.236 *Initial Detection:* 2017-08-30 17:37 UTC *Latest Detection:* 2018-04-04 08:21 UTC *Description:* The FTP server running on the remote host can be accessed using a random username and password. Nessus has enabled some countermeasures to prevent other plugins from reporting vulnerabilities incorrectly because of this.		
Network Time Protocol (NTP) Mode 6 Scanner	Medium	5.0	Restrict NTP mode 6 queries.
	1 Affected Host(s): x.x.32.33 *Initial Detection:* 2017-08-30 19:12 UTC *Latest Detection:* 2018-03-31 12:09 UTC *Description:* The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.		

Vulnerability	Severity	CVSS	Solution
PHP 5.6.x < 5.6.31 Multiple Vulnerabilities	Medium	5.0	Upgrade to PHP version 5.6.31 or later.

1 Affected Host(s): x.x.124.231
Initial Detection: 2017-11-28 18:46 UTC
Latest Detection: 2018-04-04 06:16 UTC
Description: According to its banner, the version of PHP running on the remote web server is 5.6.x prior to 5.6.31. It is, therefore, affected by the following vulnerabilities :

- An out-of-bounds read error exists in the PCRE library in the compile_bracket_matchingpath() function within file pcre_jit_compile.c. An unauthenticated, remote attacker can exploit this, via a specially crafted regular expression, to crash a process linked to the library, resulting in a denial of service condition.
(CVE-2017-6004)

- An out-of-bounds read error exists in the GD Graphics Library (LibGD) in the gdImageCreateFromGifCtx() function within file gd_gif_in.c when handling a specially crafted GIF file. An unauthenticated, remote attacker can exploit this to disclose sensitive memory contents or crash a process linked to the library.
(CVE-2017-7890)

- An out-of-bounds read error exists in Oniguruma in the match_at() function within file regexec.c. An unauthenticated, remote attacker can exploit this to disclose sensitive memory contents or crash a process linked to the library. (CVE-2017-9224)

- An out-of-bounds write error exists in Oniguruma in the next_state_val() function during regular expression compilation. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2017-9226)

- An out-of-bounds read error exists in Oniguruma in the mbc_enc_len() function within file utf8.c. An unauthenticated, remote attacker can exploit this to disclose memory contents or crash a process linked to the library. (CVE-2017-9227)

- An out-of-bounds write error exists in Oniguruma in the bitset_set_range() function during regular expression compilation. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2017-9228)

- An invalid pointer deference flaw exists in Oniguruma in the left_adjust_char_head() function within file regexec.c during regular expression compilation. An unauthenticated, remote attacker can exploit this to crash a process linked to the library, resulting in a denial of service condition. (CVE-2017-9229)

- A denial of service condition exists in PHP when handling overlarge POST requests. An unauthenticated, remote attacker can exploit this to exhaust available CPU resources. (CVE-2017-11142)

- An extended invalid free error exists in PHP in the php_wddx_push_element() function within file ext/wddx/wddx.c when parsing empty boolean tags.
An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2017-11143)

- A flaw exists in OpenSSL in the EVP_SealInit() function within file crypto/evp/p_seal.c due to returning an undocumented value of '-1'. An unauthenticated, remote attacker can exploit this to cause an unspecified impact. (CVE-2017-11144)

- An out-of-bounds read error exists in PHP in the php_parse_date() function within file ext/date/lib/parse_date.c. An unauthenti-

<table>
<tr><th>Vulnerability</th><th>Severity</th><th>CVSS</th><th>Solution</th></tr>
<tr><td>PHP 5.6.x < 5.6.32 Multiple Vulnerabilities</td><td>Medium</td><td>5.0</td><td>Upgrade to PHP version 5.6.32 or later.</td></tr>
<tr><td></td><td colspan="3"><i>1 Affected Host(s):</i> x.x.124.231
<i>Initial Detection:</i> 2017-11-28 18:46 UTC
<i>Latest Detection:</i> 2018-04-04 06:16 UTC
<i>Description:</i> According to its banner, the version of PHP running on the remote web server is 5.6.x prior to 5.6.32. It is, therefore, affected by multiple vulnerabilities.</td></tr>
<tr><td>PHP 5.6.x < 5.6.33 Multiple Vulnerabilities</td><td>Medium</td><td>5.0</td><td>Upgrade to PHP version 5.6.33 or later.</td></tr>
<tr><td></td><td colspan="3"><i>1 Affected Host(s):</i> x.x.124.231
<i>Initial Detection:</i> 2018-01-14 12:25 UTC
<i>Latest Detection:</i> 2018-04-04 06:16 UTC
<i>Description:</i> According to its banner, the version of PHP running on the remote web server is 5.6.x prior to 5.6.33. It is, therefore, affected by multiple vulnerabilities.</td></tr>
<tr><td>Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure</td><td>Medium</td><td>5.0</td><td>Upgrade to a patched version of the software. Alternatively, disable RSA key exchanges.</td></tr>
<tr><td></td><td colspan="3"><i>47 Affected Host(s):</i> x.x.165.39, x.x.80.52, x.x.81.123, x.x.81.126, x.x.81.187, x.x.83.130, x.x.83.132, x.x.83.140, x.x.83.143, x.x.83.35, x.x.83.36, x.x.84.113, x.x.84.114, x.x.84.116, x.x.84.118, x.x.84.119, x.x.84.120, x.x.84.38, x.x.84.81, x.x.84.82, x.x.84.88, x.x.84.90, x.x.84.91, x.x.84.92, x.x.84.93, x.x.85.106, x.x.85.107, x.x.85.169, x.x.85.76, x.x.85.80, x.x.85.81, x.x.85.82, x.x.85.83, x.x.85.84, x.x.85.85, x.x.85.86, x.x.85.87, x.x.87.24, x.x.90.197, x.x.90.198, x.x.90.211, x.x.91.201, x.x.92.6, x.x.92.7, x.x.93.146, x.x.93.147, x.x.93.148
<i>Initial Detection:</i> 2017-12-27 00:16 UTC
<i>Latest Detection:</i> 2018-04-04 13:11 UTC
<i>Description:</i> The remote host is affected by an information disclosure vulnerability. The SSL/TLS service supports RSA key exchanges, and incorrectly leaks whether or not the RSA key exchange sent by a client was correctly formatted. This information can allow an attacker to decrypt previous SSL/TLS sessions or impersonate the server.

Note that this plugin does not attempt to recover an RSA ciphertext, however it sends a number of correct and malformed RSA ciphertexts as part of an SSL handshake and observes how the server responds.

This plugin attempts to discover the vulnerability in multiple ways, by not completing the handshake and by completing it incorrectly, as well as using a variety of cipher suites. Only the first method that finds the service to be vulnerable is reported.</td></tr>
</table>

Vulnerability	Severity	CVSS	Solution
SSL Certificate Expiry	Medium	5.0	Purchase or generate a new SSL certificate to replace the existing one.
	61 Affected Host(s): x.x.109.229, x.x.109.230, x.x.241.232, x.x.80.167, x.x.80.170, x.x.81.187, x.x.82.147, x.x.82.194, x.x.82.195, x.x.82.196, x.x.82.199, x.x.82.201, x.x.82.202, x.x.82.203, x.x.83.140, x.x.83.89, x.x.84.81, x.x.85.122, x.x.85.145, x.x.85.162, x.x.85.163, x.x.85.168, x.x.85.176, x.x.85.5, x.x.85.72, x.x.85.75, x.x.85.78, x.x.85.79, x.x.85.85, x.x.85.86, x.x.85.87, x.x.85.88, x.x.85.89, x.x.85.90, x.x.85.91, x.x.85.94, x.x.85.95, x.x.87.227, x.x.87.228, x.x.88.178, x.x.88.179, x.x.88.180, x.x.88.182, x.x.88.183, x.x.88.185, x.x.88.186, x.x.88.187, x.x.89.41, x.x.91.159, x.x.91.162, x.x.91.163, x.x.91.164, x.x.91.165, x.x.91.200, x.x.91.208, x.x.92.80, x.x.95.100, x.x.95.101, x.x.95.102, x.x.95.108, x.x.95.29 *Initial Detection:* 2013-10-23 11:21 UTC *Latest Detection:* 2018-04-04 13:15 UTC *Description:* This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.		
SSL Certificate Signed Using Weak Hashing Algorithm	Medium	5.0	Contact the Certificate Authority to have the certificate reissued.
	72 Affected Host(s): x.x.108.25, x.x.121.222, x.x.124.236, x.x.196.117, x.x.228.130, x.x.27.11, x.x.27.34, x.x.79.162, x.x.81.187, x.x.81.241, x.x.83.35, x.x.83.36, x.x.84.145, x.x.84.88, x.x.84.90, x.x.84.91, x.x.84.92, x.x.84.93, x.x.85.123, x.x.85.132, x.x.85.139, x.x.85.140, x.x.85.141, x.x.85.142, x.x.85.155, x.x.85.159, x.x.85.30, x.x.85.32, x.x.85.5, x.x.85.76, x.x.85.85, x.x.85.86, x.x.85.87, x.x.85.89, x.x.85.9, x.x.85.90, x.x.85.91, x.x.85.93, x.x.85.94, x.x.85.95, x.x.87.26, x.x.87.61, x.x.88.189, x.x.89.40, x.x.91.147, x.x.91.156, x.x.91.159, x.x.91.167, x.x.91.168, x.x.91.169, x.x.91.175, x.x.91.192, x.x.91.193, x.x.91.194, x.x.91.196, x.x.91.197, x.x.91.236, x.x.91.249, x.x.91.254, x.x.92.81, x.x.92.82, x.x.92.83, x.x.92.84, x.x.92.85, x.x.92.86, x.x.92.87, x.x.92.88, x.x.92.90, x.x.92.91, x.x.92.92, x.x.92.94, x.x.95.26 *Initial Detection:* 2015-09-23 20:54 UTC *Latest Detection:* 2018-04-04 12:43 UTC *Description:* The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm. Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.		

Vulnerability	Severity	CVSS	Solution
SSL Medium Strength Cipher Suites Supported	Medium	5.0	Reconfigure the affected application if possible to avoid use of medium strength ciphers.

114 Affected Host(s): x.x.100.234, x.x.101.3, x.x.109.131, x.x.109.139, x.x.109.142, x.x.109.143, x.x.109.145, x.x.109.146, x.x.109.150, x.x.109.151, x.x.109.201, x.x.109.203, x.x.109.205, x.x.109.207, x.x.109.208, x.x.109.209, x.x.109.217, x.x.109.218, x.x.109.224, x.x.109.234, x.x.121.222, x.x.124.236, x.x.158.11, x.x.162.12, x.x.165.65, x.x.195.146, x.x.196.117, x.x.208.130, x.x.208.47, x.x.212.145, x.x.228.130, x.x.45.66, x.x.5.195, x.x.59.83, x.x.80.12, x.x.80.140, x.x.80.15, x.x.80.150, x.x.80.153, x.x.80.158, x.x.80.159, x.x.80.16, x.x.80.160, x.x.80.161, x.x.80.162, x.x.80.166, x.x.80.167, x.x.80.170, x.x.80.172, x.x.80.177, x.x.80.186, x.x.80.23, x.x.80.232, x.x.80.233, x.x.80.26, x.x.80.27, x.x.80.28, x.x.80.33, x.x.80.41, x.x.80.51, x.x.80.56, x.x.80.57, x.x.82.145, x.x.82.146, x.x.83.35, x.x.83.36, x.x.84.103, x.x.85.112, x.x.85.204, x.x.85.205, x.x.85.209, x.x.85.32, x.x.85.55, x.x.85.56, x.x.85.57, x.x.85.59, x.x.85.60, x.x.85.61, x.x.85.91, x.x.87.61, x.x.88.177, x.x.88.188, x.x.88.189, x.x.88.224, x.x.88.34, x.x.88.36, x.x.89.148, x.x.89.152, x.x.89.153, x.x.89.40, x.x.90.182, x.x.90.183, x.x.90.197, x.x.90.198, x.x.90.200, x.x.90.201, x.x.90.207, x.x.90.211, x.x.90.79, x.x.91.147, x.x.91.156, x.x.91.159, x.x.91.167, x.x.91.168, x.x.91.175, x.x.91.236, x.x.91.249, x.x.91.254, x.x.93.146, x.x.93.147, x.x.93.148, x.x.94.35, x.x.95.100, x.x.95.26

Initial Detection: 2016-12-08 06:26 UTC

Latest Detection: 2018-04-04 13:25 UTC

Description: The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

SSL Version 2 and 3 Protocol Detection	Medium	5.0	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.1 (with approved cipher suites) or higher instead.

11 Affected Host(s): x.x.121.222, x.x.124.236, x.x.228.130, x.x.80.158, x.x.80.167, x.x.84.103, x.x.88.189, x.x.89.40, x.x.91.236, x.x.94.35, x.x.95.26

Initial Detection: 2015-01-06 23:55 UTC

Latest Detection: 2018-04-04 08:21 UTC

Description: The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Vulnerability	Severity	CVSS	Solution
mDNS Detection (Remote Network)	Medium	5.0	Filter incoming traffic to UDP port 5353, if desired.
	1 Affected Host(s): x.x.59.83 *Initial Detection:* 2017-04-13 11:52 UTC *Latest Detection:* 2018-04-04 01:06 UTC *Description:* The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running. This plugin attempts to discover mDNS used by hosts that are not on the network segment on which Nessus resides.		
Apache Server ETag Header Information Disclosure	Medium	4.3	Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.
	1 Affected Host(s): x.x.80.186 *Initial Detection:* 2016-01-28 19:22 UTC *Latest Detection:* 2018-04-03 22:49 UTC *Description:* The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.		
HTTP TRACE / TRACK Methods Allowed	Medium	4.3	Disable these methods. Refer to the plugin output for more information.
	4 Affected Host(s): x.x.109.139, x.x.109.142, x.x.109.143, x.x.83.143 *Initial Detection:* 2014-02-04 22:36 UTC *Latest Detection:* 2018-04-03 13:39 UTC *Description:* The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.		
OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Medium	4.3	Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.
	1 Affected Host(s): x.x.84.103 *Initial Detection:* 2016-12-10 06:17 UTC *Latest Detection:* 2018-03-31 09:53 UTC *Description:* The version of OpenSSL on the remote host has been shown to allow resuming session with a weaker 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 resumptions of that session to use a weaker cipher chosen by the attacker. Note that other SSL implementations may also be affected by this vulnerability.		

Vulnerability	Severity	CVSS	Solution
SSH Weak Algorithms Supported	Medium	4.3	Contact the vendor or consult product documentation to remove the weak ciphers.
	2 Affected Host(s): x.x.105.90, x.x.157.83 *Initial Detection:* 2018-03-05 00:07 UTC *Latest Detection:* 2018-04-04 09:30 UTC *Description:* Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.		
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	4.3	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.
	61 Affected Host(s): x.x.109.139, x.x.109.142, x.x.109.143, x.x.109.201, x.x.109.203, x.x.109.205, x.x.109.207, x.x.109.209, x.x.109.217, x.x.109.218, x.x.109.224, x.x.109.234, x.x.121.222, x.x.124.236, x.x.165.65, x.x.195.146, x.x.196.117, x.x.228.130, x.x.45.66, x.x.59.83, x.x.80.153, x.x.80.159, x.x.80.160, x.x.80.162, x.x.80.166, x.x.80.170, x.x.80.172, x.x.80.177, x.x.80.186, x.x.80.23, x.x.80.26, x.x.80.27, x.x.80.28, x.x.80.33, x.x.80.51, x.x.80.56, x.x.80.57, x.x.84.103, x.x.85.204, x.x.85.205, x.x.85.209, x.x.85.32, x.x.87.61, x.x.88.188, x.x.88.189, x.x.88.224, x.x.89.40, x.x.90.183, x.x.90.79, x.x.91.147, x.x.91.156, x.x.91.159, x.x.91.167, x.x.91.168, x.x.91.175, x.x.91.236, x.x.91.249, x.x.91.254, x.x.94.35, x.x.95.100, x.x.95.26 *Initial Detection:* 2013-10-23 05:57 UTC *Latest Detection:* 2018-04-04 12:20 UTC *Description:* The remote host supports the use of RC4 in one or more cipher suites. 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.		
SSL Weak Cipher Suites Supported	Medium	4.3	Reconfigure the affected application, if possible to avoid the use of weak ciphers.
	31 Affected Host(s): x.x.109.139, x.x.109.142, x.x.109.143, x.x.109.201, x.x.109.203, x.x.109.205, x.x.109.217, x.x.109.218, x.x.109.224, x.x.109.234, x.x.121.222, x.x.124.236, x.x.80.28, x.x.84.103, x.x.85.32, x.x.87.61, x.x.88.188, x.x.88.189, x.x.89.40, x.x.90.79, x.x.91.147, x.x.91.156, x.x.91.159, x.x.91.167, x.x.91.168, x.x.91.175, x.x.91.236, x.x.91.249, x.x.91.254, x.x.95.100, x.x.95.26 *Initial Detection:* 2015-01-06 23:55 UTC *Latest Detection:* 2018-04-04 12:20 UTC *Description:* The remote host supports the use of SSL ciphers that offer weak encryption. Note: This is considerably easier to exploit if the attacker is on the same physical network.		

Vulnerability	Severity	CVSS	Solution
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Medium	4.3	Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.
	32 Affected Host(s): x.x.10.2, x.x.109.139, x.x.109.146, x.x.109.201, x.x.109.203, x.x.109.205, x.x.109.217, x.x.109.218, x.x.109.224, x.x.109.234, x.x.195.146, x.x.255.159, x.x.255.162, x.x.255.167, x.x.255.171, x.x.27.11, x.x.45.66, x.x.5.195, x.x.80.15, x.x.82.146, x.x.83.162, x.x.83.163, x.x.84.145, x.x.84.2, x.x.84.3, x.x.85.112, x.x.89.152, x.x.89.153, x.x.90.182, x.x.92.10, x.x.92.4, x.x.92.9 *Initial Detection:* 2015-05-31 01:08 UTC *Latest Detection:* 2018-04-04 13:25 UTC *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 plaintext or potentially violate the integrity of connections.		
SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)	Medium	4.3	Reconfigure the service to remove support for EXPORT_DHE cipher suites.
	1 Affected Host(s): x.x.84.103 *Initial Detection:* 2016-12-10 06:17 UTC *Latest Detection:* 2018-03-31 09:53 UTC *Description:* The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time. A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.		
SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Medium	4.3	Reconfigure the service to remove support for EXPORT_RSA cipher suites.
	19 Affected Host(s): x.x.80.28, x.x.84.103, x.x.85.32, x.x.87.61, x.x.88.188, x.x.88.189, x.x.89.40, x.x.90.79, x.x.91.147, x.x.91.156, x.x.91.159, x.x.91.167, x.x.91.168, x.x.91.175, x.x.91.236, x.x.91.249, x.x.91.254, x.x.95.100, x.x.95.26 *Initial Detection:* 2015-03-09 05:07 UTC *Latest Detection:* 2018-04-04 05:11 UTC *Description:* The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time. A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.		

Vulnerability	Severity	CVSS	Solution
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Medium	4.3	Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

8 Affected Host(s): x.x.124.236, x.x.228.130, x.x.84.103, x.x.88.189, x.x.89.40, x.x.91.236, x.x.94.35, x.x.95.26
Initial Detection: 2015-01-06 23:55 UTC
Latest Detection: 2018-04-04 08:21 UTC
Description: The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.
MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be ’rolled back’ to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents ’version rollback’ attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)	Medium	4.3	Contact the vendor for an update.

2 Affected Host(s): x.x.10.2, x.x.228.130
Initial Detection: 2015-07-05 21:56 UTC
Latest Detection: 2018-04-04 12:59 UTC
Description: The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the TLS server not verifying block cipher padding when using a cipher suite that employs a block cipher such as AES and DES. The lack of padding checking can allow encrypted TLS traffic to be decrypted. This vulnerability could allow for the decryption of HTTPS traffic by an unauthorized third party.

Vulnerability	Severity	CVSS	Solution
Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Medium	4.3	Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.
	1 Affected Host(s): x.x.108.25 *Initial Detection:* 2018-03-05 00:10 UTC *Latest Detection:* 2018-03-30 00:33 UTC *Description:* The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.		
Terminal Services Encryption Level is Medium or Low	Medium	4.3	Change RDP encryption level to one of : 3. High 4. FIPS Compliant
	1 Affected Host(s): x.x.108.25 *Initial Detection:* 2018-03-05 00:10 UTC *Latest Detection:* 2018-03-30 00:33 UTC *Description:* The remote Terminal Services service is not configured to use strong cryptography. Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.		

Vulnerability	Severity	CVSS	Solution
Web Application Potentially Vulnerable to Clickjacking	Medium	4.3	Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.
	10 Affected Host(s): x.x.109.217, x.x.109.218, x.x.109.221, x.x.109.234, x.x.12.165, x.x.124.231, x.x.255.159, x.x.81.126, x.x.81.241, x.x.83.130 *Initial Detection:* 2017-09-14 21:16 UTC *Latest Detection:* 2018-04-04 11:07 UTC *Description:* The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions. X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors. Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource. Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.		
Web Server Generic Cookie Injection	Medium	4.3	Contact the vendor for a patch or upgrade.
	2 Affected Host(s): x.x.87.202, x.x.87.205 *Initial Detection:* 2017-03-05 16:01 UTC *Latest Detection:* 2018-04-03 13:51 UTC *Description:* The remote host is running a web server that fails to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to inject arbitrary cookies. Depending on the structure of the web application, it may be possible to launch a 'session fixation' attack using this mechanism. Please note that : - Nessus did not check if the session fixation attack is feasible. - This is not the only vector of session fixation.		

Vulnerability	Severity	CVSS	Solution
Web Server Generic XSS	Medium	4.3	Contact the vendor for a patch or upgrade.
	3 Affected Host(s): x.x.196.117, x.x.87.202, x.x.87.205 *Initial Detection:* 2017-09-15 19:49 UTC *Latest Detection:* 2018-04-03 20:08 UTC *Description:* The remote host is running a web server that fails to adequately sanitize request strings of malicious JavaScript. A remote attacker can exploit this issue, via a specially crafted request, to execute arbitrary HTML and script code in a user's browser within the security context of the affected site.		
OpenSSL 1.1.0 < 1.1.0g RSA/DSA Unspecified Carry Issue	Medium	4.0	Upgrade to OpenSSL version 1.1.0g or later.
	1 Affected Host(s): x.x.80.193 *Initial Detection:* 2017-11-07 07:35 UTC *Latest Detection:* 2018-04-02 10:31 UTC *Description:* According to its banner, the version of OpenSSL running on the remote host is 1.1.0 prior to 1.1.0g. It is, therefore, affected by an unspecified carry vulnerability.		
MikroTik RouterOS < 6.39.3 / 6.40.4 / 6.41rc (KRACK)	Low	2.9	Upgrade to MikroTik RouterOS 6.39.3 / 6.40.4 / 6.41rc or later.
	1 Affected Host(s): x.x.236.156 *Initial Detection:* 2018-03-04 21:53 UTC *Latest Detection:* 2018-04-04 11:56 UTC *Description:* According to its self-reported version, the remote networking device is running a version of MikroTik 6.9.X prior to 6.39.3, 6.40.x < 6.40.4, or 6.41rc. It, therefore, vulnerable to multiple vulnerabilities discovered in the WPA2 handshake protocol.		
FTP Supports Cleartext Authentication	Low	2.6	Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.
	3 Affected Host(s): x.x.124.226, x.x.193.95, x.x.59.81 *Initial Detection:* 2017-03-06 19:26 UTC *Latest Detection:* 2018-04-03 14:33 UTC *Description:* The remote FTP server allows the user's name and password to be transmitted in cleartext, which could be intercepted by a network sniffer or a man-in-the-middle attack.		
OpenSSL AES-NI Padding Oracle MitM Information Disclosure	Low	2.6	Upgrade to OpenSSL version 1.0.1t / 1.0.2h or later.
	1 Affected Host(s): x.x.124.226 *Initial Detection:* 2017-08-30 17:28 UTC *Latest Detection:* 2018-04-02 02:11 UTC *Description:* The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability due to an error in the implementation of ciphersuites that use AES in CBC mode with HMAC-SHA1 or HMAC-SHA256. The implementation is specially written to use the AES acceleration available in x86/amd64 processors (AES-NI). The error messages returned by the server allow allow a man-in-the-middle attacker to conduct a padding oracle attack, resulting in the ability to decrypt network traffic.		

Vulnerability	Severity	CVSS	Solution
POP3 Cleartext Logins Permitted	Low	2.6	Contact your vendor for a fix or encrypt traffic with SSL / TLS using stunnel.
	1 Affected Host(s): x.x.59.83 *Initial Detection:* 2017-04-13 11:52 UTC *Latest Detection:* 2018-04-04 01:06 UTC *Description:* The remote host is running a POP3 daemon that allows cleartext logins over unencrypted connections. An attacker can uncover user names and passwords by sniffing traffic to the POP3 daemon if a less secure authentication mechanism (eg, USER command, AUTH PLAIN, AUTH LOGIN) is used.		
SSH Server CBC Mode Ciphers Enabled	Low	2.6	Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.
	11 Affected Host(s): x.x.105.90, x.x.127.185, x.x.157.83, x.x.174.177, x.x.194.170, x.x.236.156, x.x.32.33, x.x.83.74, x.x.84.50, x.x.89.182, x.x.89.194 *Initial Detection:* 2014-02-03 16:26 UTC *Latest Detection:* 2018-04-04 11:56 UTC *Description:* The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext. Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.		
SSH Weak MAC Algorithms Enabled	Low	2.6	Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.
	9 Affected Host(s): x.x.105.90, x.x.157.83, x.x.194.170, x.x.236.156, x.x.32.33, x.x.83.74, x.x.84.50, x.x.89.182, x.x.89.194 *Initial Detection:* 2014-02-03 16:26 UTC *Latest Detection:* 2018-04-04 11:56 UTC *Description:* The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak. Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.		
Terminal Services Encryption Level is not FIPS-140 Compliant	Low	2.6	Change RDP encryption level to : 4. FIPS Compliant
	1 Affected Host(s): x.x.108.25 *Initial Detection:* 2018-03-05 00:10 UTC *Latest Detection:* 2018-03-30 00:33 UTC *Description:* The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.		

Vulnerability	Severity	CVSS	Solution
Web Server HTTP Header Internal IP Disclosure	Low	2.6	None
	2 Affected Host(s): x.x.158.25, x.x.82.145 *Initial Detection:* 2017-01-09 09:47 UTC *Latest Detection:* 2018-04-02 00:11 UTC *Description:* This may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall or proxy server. There is a known issue with Microsoft IIS 4.0 doing this in its default configuration. This may also affect other web servers, web applications, web proxies, load balancers and through a variety of misconfigurations related to redirection.		
Web Server Load Balancer Detection	Low	2.6	Update the web configuration to hide information disclosure.
	1 Affected Host(s): x.x.93.146 *Initial Detection:* 2015-04-08 08:54 UTC *Latest Detection:* 2018-03-31 13:17 UTC *Description:* The remote web server seems to be running in conjunction with several others behind a load balancer. Knowing that there are multiple systems behind a service could be useful to an attacker as the underlying hosts may be running different operating systems, patchlevels, etc.		
Web Server Transmits Cleartext Credentials	Low	2.6	Make sure that every sensitive form transmits content over HTTPS.
	38 Affected Host(s): x.x.124.231, x.x.157.83, x.x.192.133, x.x.192.16, x.x.192.20, x.x.193.12, x.x.193.130, x.x.193.138, x.x.193.149, x.x.193.95, x.x.194.150, x.x.194.170, x.x.194.188, x.x.194.196, x.x.194.207, x.x.194.79, x.x.195.142, x.x.195.145, x.x.195.208, x.x.195.245, x.x.196.10, x.x.196.119, x.x.196.134, x.x.196.194, x.x.196.200, x.x.196.250, x.x.196.253, x.x.196.93, x.x.196.94, x.x.196.96, x.x.197.23, x.x.197.47, x.x.41.161, x.x.41.166, x.x.41.168, x.x.41.180, x.x.52.235, x.x.9.184 *Initial Detection:* 2017-11-28 18:46 UTC *Latest Detection:* 2018-04-04 13:35 UTC *Description:* The remote web server contains several HTML form fields containing an input of type ’password’ which transmit their information to a remote web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.		
Web Server Uses Basic Authentication Without HTTPS	Low	2.6	Make sure that HTTP authentication is transmitted over HTTPS.
	6 Affected Host(s): x.x.124.231, x.x.157.83, x.x.194.196, x.x.195.142, x.x.196.250, x.x.59.81 *Initial Detection:* 2017-11-28 18:46 UTC *Latest Detection:* 2018-04-04 10:41 UTC *Description:* The remote web server contains web pages that are protected by ’Basic’ authentication over cleartext. An attacker eavesdropping the traffic might obtain logins and passwords of valid users.		

Vulnerability	Severity	CVSS	Solution
Dropbear SSH Server < 2016.72 Multiple Vulnerabilities	Low	2.1	Upgrade to Dropbear SSH version 2016.74 or later.
	1 Affected Host(s): x.x.194.170 *Initial Detection:* 2018-03-04 21:23 UTC *Latest Detection:* 2018-04-03 01:06 UTC *Description:* According to its self-reported version in its banner, Dropbear SSH running on the remote host is prior to 2016.74. It is, therefore, affected by the following vulnerabilities : - A format string flaw exists due to improper handling of string format specifiers (e.g., %s and %x) in usernames and host arguments. An unauthenticated, remote attacker can exploit this to execute arbitrary code with root privileges. (CVE-2016-7406) - A flaw exists in dropbearconvert due to improper handling of specially crafted OpenSSH key files. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-7407) - A flaw exists in dbclient when handling the -m or -c arguments in scripts. An unauthenticated, remote attacker can exploit this, via a specially crafted script, to execute arbitrary code. (CVE-2016-7408) - A flaw exists in dbclient or dropbear server if they are compiled with the DEBUG_TRACE option and then run using the -v switch. A local attacker can exploit this to disclose process memory. (CVE-2016-7409)		
Anonymous FTP Enabled	Low	0.0	Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure that sensitive content is not being made available.
	2 Affected Host(s): x.x.124.236, x.x.184.204 *Initial Detection:* 2017-04-19 12:21 UTC *Latest Detection:* 2018-04-04 08:21 UTC *Description:* Nessus has detected that the FTP server running on the remote host allows anonymous logins. Therefore, any remote user may connect and authenticate to the server without providing a password or unique credentials. This allows the user to access any files made available by the FTP server.		

Vulnerability	Severity	CVSS	Solution
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	Low	0.0	Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.
	24 Affected Host(s): x.x.121.222, x.x.196.117, x.x.228.130, x.x.27.34, x.x.84.145, x.x.85.162, x.x.85.163, x.x.85.72, x.x.85.75, x.x.85.78, x.x.85.79, x.x.85.88, x.x.85.9, x.x.88.189, x.x.89.40, x.x.89.41, x.x.91.162, x.x.91.163, x.x.91.164, x.x.91.165, x.x.91.236, x.x.92.80, x.x.95.100, x.x.95.26 *Initial Detection:* 2013-10-23 11:21 UTC *Latest Detection:* 2018-04-04 13:15 UTC *Description:* At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits. Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014. Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.		

Appendix D Critical and High Vulnerability Mitigations by IP Address

This section presents detailed scan results, ordered by host, from the network mapping and vulnerability scans. The table only displays high and critical vulnerabilities. Vulnerabilities identified have a recommended mitigation solution that should be considered in order to establish or maintain a secure network.

Owner	Host	Port(s)	Vulnerability	Severity	Age Days	Solution
SUB_ORG	x.x.105.90	NA	MikroTik RouterOS < 6.41.3 SMB Buffer Overflow	Critical	12	Upgrade to MikroTik RouterOS 6.41.3 or later.
SUB_ORG	x.x.157.83	NA	MikroTik RouterOS < 6.41.3 SMB Buffer Overflow	Critical	11	Upgrade to MikroTik RouterOS 6.41.3 or later.
SUB_ORG	x.x.192.34	NA	MikroTik RouterOS < 6.41.3 SMB Buffer Overflow	Critical	11	Upgrade to MikroTik RouterOS 6.41.3 or later.
SUB_ORG	x.x.236.156	NA	MikroTik RouterOS < 6.41.3 SMB Buffer Overflow	Critical	11	Upgrade to MikroTik RouterOS 6.41.3 or later.
SUB_ORG	x.x.105.90	8090	MikroTik RouterOS HTTP Server Arbitrary Write RCE (ChimayRed)	Critical	30	Upgrade to MikroTik RouterOS version 6.38.5 or later.
SUB_ORG	x.x.157.83	8090	MikroTik RouterOS HTTP Server Arbitrary Write RCE (ChimayRed)	Critical	29	Upgrade to MikroTik RouterOS version 6.38.5 or later.
SUB_ORG	x.x.192.34	8090	MikroTik RouterOS HTTP Server Arbitrary Write RCE (ChimayRed)	Critical	30	Upgrade to MikroTik RouterOS version 6.38.5 or later.
SUB_ORG	x.x.194.150	49152	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE	Critical	30	Upgrade to libupnp version 1.6.18 or later. If libupnp is used as a third party library by a different application, contact the vendor of that application for a fix.
SUB_ORG	x.x.196.200	49152	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE	Critical	30	Upgrade to libupnp version 1.6.18 or later. If libupnp is used as a third party library by a different application, contact the vendor of that application for a fix.
SUB_ORG	x.x.196.96	49152	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE	Critical	31	Upgrade to libupnp version 1.6.18 or later. If libupnp is used as a third party library by a different application, contact the vendor of that application for a fix.
SUB_ORG	x.x.124.236	21	FTP Privileged Port Bounce Scan	High	212	See the CERT advisory in the references for solutions and workarounds.
SUB_ORG	x.x.124.231	80	PHP 5.6.x < 5.6.34 Stack Buffer Overflow	High	23	Upgrade to PHP version 5.6.34 or later.
SUB_ORG	x.x.124.231	443	PHP 5.6.x < 5.6.34 Stack Buffer Overflow	High	25	Upgrade to PHP version 5.6.34 or later.
SUB_ORG	x.x.175.46	161	SNMP Agent Default Community Name (public)	High	87	Disable the SNMP service on the remote host if you do not use it. Either filter incoming UDP packets going to this port, or change the default community string.

Appendix E False Positive Findings

This section lists findings that SAMPLE asserted to NCATS to be false positive (i.e., data that incorrectly indicates a vulnerability is present). If SAMPLE would like to report findings for false positive consideration, please submit an email through your designated technical point of contact with an analysis and evidence indicating how SAMPLE determined the finding is a false positive. Unless NCATS determines the submission is insufficient, NCATS will leave the determination for what constitutes a false positive to report recipients. False positive status expires by default 365 days after the false positive was marked as such by NCATS. When a finding's false positive status expires, the finding will be removed from this section. If the finding is then re-detected, its status should be reviewed.

E.1 Expiring Soon False Positive Findings

This section lists false positive findings whose status as a false positive is expiring within 30 days. If SAMPLE would like to extend the expiration date of a false positive, please submit an email through your designated technical point of contact with an analysis and evidence indicating how SAMPLE determined the finding is still considered a false positive. For a full listing of false positives, please see Appendix E.2: All False Positive Findings.

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Latest Detection	False Positive	False Positive
					(UTC)	(UTC)	Effective	Expiration

There are currently no false positive findings that will expire in the next 30 days.

E.2 All False Positive Findings

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Latest Detection	False Positive	False Positive
					(UTC)	(UTC)	Effective	Expiration
SUB_ORG	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	Critical	x.x.85.185	443	2017-05-10 15:59	2018-02-25 16:51	2017-05-22	2018-05-22

Appendix F Frequently Asked Questions

This section seeks to answer the most frequently asked questions about Cyber Hygiene reports.

1. **I think the vulnerability listed in my report is a false positive. Can you remove it from my report?**

   - If you believe a finding to be in error, you can submit a false positive assertion to ncats@hq.dhs.gov which should include the following:
     - the name of the vulnerability,
     - IP address and port, and
     - your analysis and supporting evidence.

     NCATS will review and perform our own analysis. This will not include exploiting a vulnerability, but may include actively sending packets to the host in question.
   - If our research appears to confirm your analysis, the vulnerability will be marked as a false positive for that host and will stop appearing in the main body of report for one year. Vulnerabilities marked as ’false positive’ will be reported in Appendix E: False Positive Findings, along with the name and date of the individual who submitted the request to us.
   - NCATS reserves the right to assert that certain findings are not false positives, and when false positive assertions are accepted by NCATS, that acceptance should not be construed as validation that a finding is in fact a false positive.

2. **Can I get the data you created this report from in CSV?**

   - Certainly! See Appendix G: Attachments.

3. **I fixed a vulnerability listed in my report. Can you rescan to verify?**

   - CyHy automatically rescans whenever a vulnerability is detected, so there is no need to notify us that you’ve fixed something. If we can no longer detect the vulnerability, it will be listed in Appendix B.1: Mitigated Vulnerabilities.

4. **The DHS Binding Operational Directive 15-01 (BOD) requires my agency to fix Critical vulnerabilities within 30 days. If we can’t do that, who do we contact and what needs to be sent?**

   - For all questions or submissions related to the BOD, please email fnr.bod@hq.dhs.gov.
   - To be clear, if a Critical vulnerability
     - is less than 30 days old and your agency can fix it before it hits 30 days old, nothing needs to be sent to DHS.
     - can’t or won’t be fixed within 30 days (or it’s already older than 30 days), send fnr.bod@hq.dhs.gov a Plan Of Action and Milestones (POA&M) that includes the following information:
       (a) a detailed justification outlining any barriers to expedited mitigation,
       (b) the steps you are taking to get to a resolution, and
       (c) a timeframe for mitigation.
   - Remediation of the Critical vulnerability will be validated when our scans no longer detect the vulnerability, not through an assessment of or concurrence with your submitted POA&M. Even with the submission of a POA&M, the vulnerability will continue to be listed on your CyHy report until remediated (i.e., it will not be marked as a false positive).

5. **Can I add my third-party hosted/managed servers?**

   - Yes, and we recommend that you do so, but we request that you obtain authorization/consent before we begin scanning them. DHS does not require documentation from your third-parties.

6. **Why do the host counts in my Cyber Hygiene report not match the number of known Internet-facing end points on my network?**

   - This is likely due to a difference in what we’re defining as a host. CyHy considers a device a host if there is at least one open port/service operating at the address. When we scan, any number of things can occur that make it appear that nothing is at that address (e.g., our scans are blocked by host or network filters, the device is down for maintenance, packets are dropped or lost en route, etc.).

- If a port is detected as 'tcpwrapped', it means that the TCP handshake was completed, but the connection was closed before any data was sent back. For the purposes of this report, tcpwrapped ports are not considered to be 'open'. If a device only responds with tcpwrapped ports, then it will not be considered a host by CyHy. For more information about tcpwrapped ports, see https://secwiki.org/w/FAQ_tcpwrapped.
- The intent of CyHy is to find vulnerabilities, not count hosts, and our metrics should not be relied upon as a verified host count of your organization. The weekly host count should be taken as an estimate. If, however, there are no or extremely low host counts reported when there are known active hosts, it is possible that the CyHy scans are being blocked.

7. **I've added a new host and your scans are not picking it up.**

   - CyHy is not scanning your entire IP scope every week. If you've stood up a new server in a range that we only recently scanned and found nothing in, it's possible that the new server would not appear for nearly 90 days. If you want the new host to be scanned immediately, you can email ncats@hq.dhs.gov and we'll manually scan it, which will add it to your weekly report.

8. **I'm getting SSL/TLS certificate vulnerabilities that I think are incorrect.**

   - In our scans, we will use the Mozilla trust store. NCATS will not accept any other roots. This is done as a matter of practice and principle: as practice, because maintaining private roots from our various stakeholders is operationally infeasible; as principle, because our scans aim to ensure that the user of your services is protected. The Mozilla trust store is generally representative of a 'lowest common denominator' in what a public-serving site can reasonably expect of those users whose devices they do not manage.
   - Ensure that the root your certificate is issued from is included in the Mozilla root store. You should also verify that the intermediate certificates are presented with your site certificate. This allows the scanner to validate the certificate's chain of trust.
   - Though the site is Federal Government-centric, tons of great information can be found at https.cio.gov regarding Hypertext Transfer Protocol Secure (HTTPS), much of which is applicable for SSL/TLS more generally.

9. **What do the different appendices represent? How can a vulnerability be in more than one appendix? Which vulnerabilities are counted in the Report Card?**

Vulnerability Type	Counted in	Listed in Appendix					
	Report Card?	A	B.1	B.2	B.3	B.4	C
Detected in latest scan, for the first time (i.e. "brand new vulnerability")	Yes	✓		✓			✓
Re-detected in latest scan (previously reported; was present in last week's Appendix A and C)	Yes	✓					✓
Re-detected in latest scan (previously reported and mitigated; was NOT present in last week's Appendix A and C)	Yes	✓			✓		✓
Reported last week in Appendix A and C, but not detected since then (i.e. "currently mitigated")	No		✓				
Not detected in latest scan, but detected at some point between last report and latest scan	No					✓	

10. **Can you scan my IPv6 addresses?**

    - There is currently no ETA for CyHy to scan IPv6 addresses.

11. **Can you scan this list of domains for me?**

    - For vulnerability scanning, CyHy does not presently scan domain names directly, but we expect to do so in FY18.

12. **How can I change who receives my Cyber Hygiene report?**

    - The CyHy report will be delivered to a single address. Most organizations set up a distribution address which takes incoming mail and delivers it to individual mailboxes. NCATS strongly recommends this approach because it allows your organization to grant access to the report to whomever you'd like, as well as manage the change control of employees onboarding or leaving. If you need to change the distro we mail to, email us at ncats@hq.dhs.gov.

13. **Can I change the password for my report?**

- If you need to request a new password for your report, email us at ncats@hq.dhs.gov. Please let us know if you'd like the password texted, delivered over the phone (note if voicemail is ok), or just emailed back.

14. **How is the age of each vulnerability calculated?**

    - Vulnerability age is determined by when it was first detected on a host, not from when it first appeared on a report. For more information, refer to the "Recurring Vulnerabilities" paragraph in Section 5.2: Methodology / Process.

Appendix G Attachments

If your PDF viewer supports embedded attachments you will see paperclip icons below for each attached file.

- 📎 findings.csv : Detailed list of all vulnerability findings for each IP address and port.
- 📎 mitigated-vulnerabilities.csv : List of vulnerabilities that were included on the last report, but were not detected in the latest scans.
- 📎 recently-detected.csv : List of all vulnerabilities detected since the last report, but not detected in the latest scans.
- 📎 services.csv : List of all discovered services and the associated IP address and port. NOTE: This attachment excludes the 63,276 service(s) detected as ’tcpwrapped’, which indicates that a full TCP handshake was completed, but the connection was closed before any data was sent. For more information, refer to the Frequently Asked Questions section.
- 📎 hosts.csv : List of hosts discovered with IP address, best-guess OS identification, and hostname if available.
- 📎 scope.csv : List of IP addresses that were in scope for this report.
- 📎 false-positive-findings.csv : List of all reported false positive vulnerability findings.
- 📎 sub-org-summary.csv : Data from the Sub-Organization Summary.
- 📎 days-to-mitigate.csv: Metrics over time for median and maximum days to mitigate findings (calculated with vulnerabilities mitigated since date listed in each row).
- 📎 days-currently-active.csv: Metrics over time for median and maximum age of active vulnerabilities (active as of date listed in each row).

Appendix H Glossary and Acronyms

Glossary

active vulnerability A vulnerability that was detected in the most recent scan of a host used for this report. 8, 15

false positive Any normal or expected behavior that is identified in this report as a potentially exploitable vulnerability. 7, 15, 70, 71, 74

host A device that has a least one open port/listening service. 5, 7, 11, 12, 14–16, 19, 69, 71, 74

initial detection The initial point in time when Cyber Hygiene scans identified a vulnerability. This date is used to calculate the vulnerability's age. 8, 9, 12, 23, 32, 36

IP address A numerical label that identifies each device using the Internet Protocol to communicate over a network. 71

latest detection The most recent time when Cyber Hygiene scans identified a particular vulnerability. 32, 36

mitigation detection The date when a previously identified vulnerability was no longer detected by Cyber Hygiene scans. 23

service An application running at the network application layer that provides communications capabilities across an IP computer network. 5, 11, 12, 18, 74

severity Please review the following guide for vulnerability severity scoring information: https://www.first.org/cvss/v2/guide. 5, 12, 16, 19, 21

vulnerability A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. 5, 7–9, 11, 12, 15, 16, 18–21, 23, 32, 36, 44, 69–71, 74

vulnerability age The time between a vulnerability's initial detection date and its latest detection date. 8, 9, 12, 73

vulnerable host A host with at least one vulnerability detected on the most recent scan used for this report. 19

Acronyms

CS&C Office of Cybersecurity and Communications [https://www.dhs.gov/office-cybersecurity-and-communications]. 11

CSV Comma-Separated Values. 5, 10, 11, 71

CVE Common Vulnerabilities and Exposures; for more information refer to https://cve.mitre.org/about/faqs.html. 13

CVSS Common Vulnerability Scoring System; for more information refer to https://www.first.org/cvss/v2. 4, 13, 15, 16

CyHy Cyber Hygiene. 5, 7–11, 13, 15, 17, 71, 72

DHS Department of Homeland Security [https://www.dhs.gov]. 5, 7, 11, 71

HTTPS Hypertext Transfer Protocol Secure. 72

IP Internet Protocol. 11, 72, 74

IT Information Technology. 7

NCATS National Cybersecurity Assessments and Technical Services. 7, 11, 12, 15, 20, 70–72

NCCIC National Cybersecurity and Communications Integration Center [https://www.dhs.gov/about-national-cybersecurity-communications-integration-center]. 11

NPPD National Protection and Programs Directorate [https://www.dhs.gov/national-protection-and-programs-directorate]. 11

NVD National Vulnerability Database; for more information refer to https://nvd.nist.gov. 13

OS Operating System. 11, 74

POA&M Plan Of Action and Milestones. 71

RRS Risk Rating System. 16

SAMPLE Sample Organization. 5, 7–11, 14, 15, 18–20, 70

TCP Transmission Control Protocol. 11