ASSESSMENT SUMMARY

Cyber Hygiene Assessment

CYHY NUMBER

February 4, 2024 DATE

Cyber Hygiene Assessment

Sample Organization

CISA
CYBER+INFRASTRUCTURE

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. Review the Emergency Directive 19-01 — New Certificates Summary for current certificate information. This section gives a quick look at the currently expired, soon to expire, and newly added certificates for known hostnames owned by or managed on behalf of your organization.
3. 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.
4. 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.
5. 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 February 4, 2024.
6. 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.
7. Review Appendix E: False Positive Findings to track any upcoming expiration dates for false positive designations. For any new false positives, please complete and return the False Positive Assertion Form found in Appendix G: Attachments to the Cybersecurity and Infrastructure Security Agency (CISA).

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 vulnerability@cisa.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, the CISA 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
Technical	Technical POC 3	tech_poc_3@sample.org	555-555-3333
Technical	Technical POC 4	tech_poc_4@sample.org	555-555-4444
Distribution List	Distro POC 1	distro_poc_1@sample.org	

2024-02-04

CYBER HYGIENE

REPORT CARD

Sample Organization

0
Hosts with unsupported software

37
Potentially Risky Open Services

3%
Decrease in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

November 6, 2023 — February 4, 2024
Completed host scan on all assets

January 26, 2024 — February 4, 2024
Last vulnerability scan on all hosts

ASSETS OWNED

220,807
No Change

ASSETS SCANNED

220,807
No Change
100% of assets scanned

HOSTS

827
Decrease of **10**

SERVICES

2,413
Increase of **33**

VULNERABLE HOSTS

268
Decrease of **6**
32% of hosts vulnerable

VULNERABILITIES

896
Decrease of **6**

VULNERABILITIES

SEVERITY BY PROMINENCE

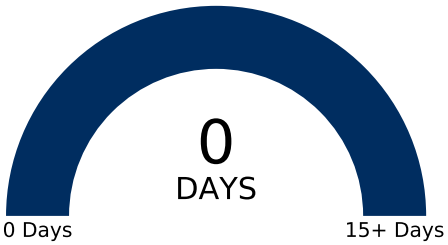
0 CRITICAL
3 RESOLVED
0 NEW

4 HIGH
0 RESOLVED
0 NEW

841 MEDIUM
20 RESOLVED
18 NEW

51 LOW
6 RESOLVED
5 NEW

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS

MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0	FTP 4
Telnet* 11	RPC 1
SMB* 0	SQL 4
LDAP 0	IRC 0
NETBIOS 3	Kerberos 14

None Open · Open, No New · Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

** Denotes the possibility of a network management interface.*

3 Binding Operational Directive 22-01 — Reducing the Significant Risk of Known Exploited Vulnerabilities

Malicious cyber campaigns frequently use Known Exploited Vulnerabilities (KEVs) to threaten the public sector, the private sector, and ultimately the security and privacy of individual citizens. Therefore it is essential to quickly remediate KEVs to protect federal information systems and reduce cyber incidents.

CISA issued Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilties to evolve the federal government's approach to vulnerability management and keep pace with threat activity. The directive establishes a CISA managed catalog of known exploited vulnerabilities and requires federal civilian agencies to identify and remediate these vulnerabilities found on your information systems within two weeks.

CISA updates this catalog with new vulnerabilities when the following conditions are met:

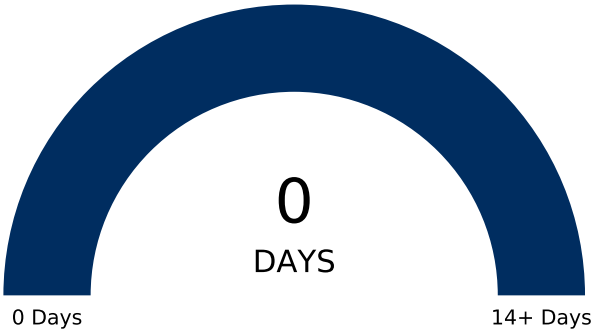
- The vulnerability has an assigned Common Vulnerabilities and Exposures (CVE) ID.
- There is reliable evidence that the vulnerability has been actively exploited in the wild.
- There is a clear remediation action for the vulnerability, such as a vendor provided update.

To report newly exploited vulnerabilities that are not in this catalog, please email CISA Central at central@cisa.dhs.gov.

Details on the below findings can be found in "findings.csv" in Appendix G.

KEV SEVERITY BY PROMINENCE

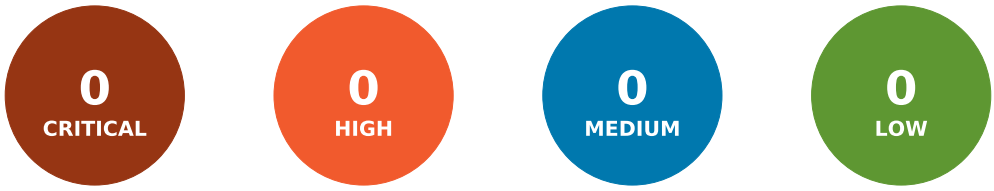
KEV RESPONSE TIME



MAX AGE OF ACTIVE KEVS

Signed into law in March 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) required CISA to establish the Ransomware Vulnerability Warning Pilot (RVWP). The goal of the RVWP is to warn organizations about exposed vulnerabilities that may be exploited by ransomware threat actors.

Of the **0** KEV findings detected on SAMPLE's internet-facing assets, **0** are known by CISA to have been used in ransomware campaigns.



4 Binding Operational Directive 23-02 — Mitigating the Risk from Internet-Exposed Management Interfaces

Threat actors often use certain classes of network devices to gain unrestricted access to organizational networks leading to full scale compromises. Inadequate security, misconfigurations, and out-of-date software make these devices more vulnerable to exploitation. The risk is further compounded if device management interfaces are connected directly to, and accessible from, the public-facing Internet. Most device management interfaces are designed to be accessed from dedicated physical interfaces and/or management networks and are not meant to be accessible directly from the public Internet.

CISA issued Binding Operational Directive (BOD) 23-02 to push the federal government to take steps toward reducing the attack surface created by insecure or misconfigured management interfaces across certain classes of devices. The BOD requires networked management interfaces (NMIs) using certain protocols over the Internet to be removed from the public Internet or to be protected by capabilities that enforce access control to the interface through a policy enforcement point separate from the interface itself as part of a Zero Trust Architecture (ZTA) within 14 days of discovery.

We also recommend reviewing all hosts with potentially risky open services, especially if they are functioning as networked management interfaces, to ensure that each service is intended to be available to the public and, where applicable, the service is up to date on the latest version, correctly configured, and uses strong authentication.

You can find a list of potentially risky services detected as available on your external network within this report's "potentially-risky-services.csv" attachment. In it, there is a column which denotes those that may be associated with NMIs to help with prioritization.

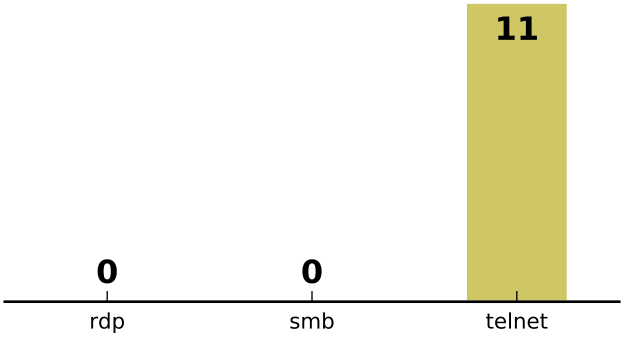


Figure 1: Potential Network Management Interface (NMI) Service Counts

The details for these findings can be found within the "potentially-risky-services.csv" file located in Appendix G: Attachments. You will need to ensure you open the report with a dedicated PDF reader (such as Adobe Acrobat), and click on the paper clip icon to the left of the CSV file in order to open it.

5 Emergency Directive 19-01 — New Certificates Summary

Issued on 22 January 2019, Emergency Directive (ED) 19-01 requires CISA to assist Federal agencies in identifying newly added certificates to Certificate transparency (CT) logs for agency domains. CISA is supporting the directive by providing certificate information found in CT log entries for known agency second-level domains and all subdomains under them. Per the directive, agencies shall monitor CT log data for certificates issued that they did not request. Detailed information on the certificates discovered by CISA can be found in the `certificates.csv` attachment within the agency's weekly Cyber Hygiene report.

We recommend focusing on validating that newly-added certificates were purposefully issued; new certificates issued without a known purpose may indicate Domain Name Service (DNS) infrastructure tampering. The issuing organization table is included to help identify possible outlier certificates that have been issued by an unusual organization.

HIGH LEVEL FINDINGS

UNEXPIRED CERTIFICATES	LATEST SCAN DATE
47	February 4, 2024

NEW CERTIFICATES ISSUED

CURRENT FISCAL YEAR	LAST 30 DAYS	LAST 7 DAYS
50	20	7

CERTIFICATE EXPIRATION

EXPIRED IN LAST 7 DAYS	EXPIRED IN LAST 30 DAYS	EXPIRING IN 7 DAYS	EXPIRING IN 30 DAYS
2	12	4	11

Issuing Agency	Number of Certificates
CN=R3,O=Let's Encrypt,C=US	17
CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	7
CN=E1,O=Let's Encrypt,C=US	7
CN=GTS CA 1P5,O=Google Trust Services LLC,C=US	6
CN=Sectigo ECC Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	6
CN=Amazon RSA 2048 M02,O=Amazon,C=US	1
CN=Entrust Certification Authority - L1K,OU=(c) 2012 Entrust\, Inc. - for authorized use only,OU=See www.entrust.net/legal-terms,O=Entrust\, Inc.,C=US	1
CN=GeoTrust RSA CA 2018,OU=www.digicert.com,O=DigiCert Inc,C=US	1
CN=DigiCert EV RSA CA G2,O=DigiCert Inc,C=US	1

6 Executive Summary

This report provides the results of a CISA CyHy assessment of SAMPLE conducted from November 6, 2023 at 15:42 UTC through February 4, 2024 at 17:33 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 827 hosts were identified out of the 220,807 addresses provided to CISA. The scanning revealed 896 total potential vulnerabilities on 268 vulnerable hosts, 32% of all SAMPLE hosts. 258 distinct open ports, 183 distinct services, and 64 operating systems were detected.

30 distinct types of potential vulnerabilities (0 critical, 2 high, 20 medium, and 8 low) were detected, as shown in Table 2. The vulnerabilities that were detected most frequently on SAMPLE hosts are displayed in Figure 2.

SAMPLE should review the potential vulnerabilities detected and report any false positives back to CISA 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	0%	0	0%	0
High	7%	2	0%	4
Medium	67%	20	94%	841
Low	27%	8	6%	51
Total		30		896

Table 2: Number of Vulnerabilities by Severity Level

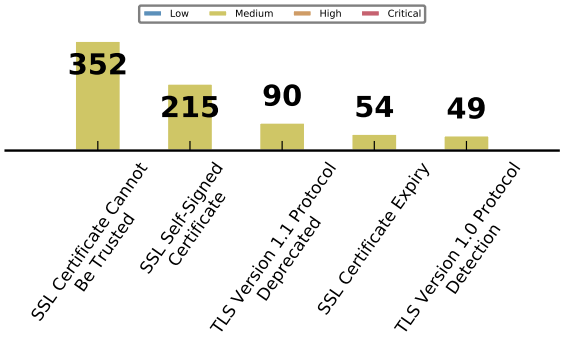


Figure 2: Top Vulnerabilities by Occurrence

Additionally, the top high-risk hosts and top risk-based vulnerabilities are displayed in Figure 3 and Figure 4. For more information about these risk calculations, refer to Table 9: Risk Rating System.

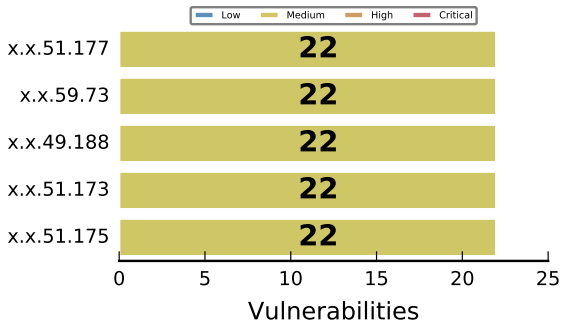


Figure 3: Top High-Risk Hosts

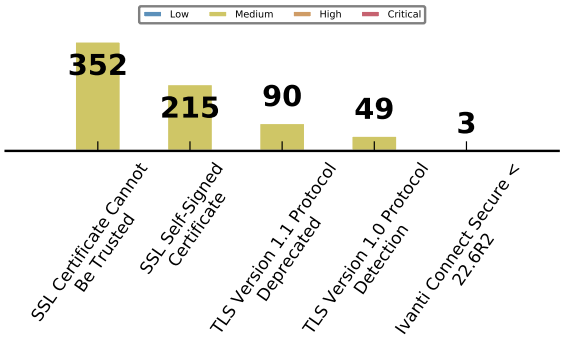


Figure 4: Top Risk-Based Vulnerabilities

⚠ 7 false positive finding(s) expire within 30 days.
See Appendix E.1: Expiring Soon False Positive Findings for more information.

The most frequently detected operating systems and services for SAMPLE are displayed in Table 3 and Table 4 respectively.

Operating System	Detections	
unknown	63.1%	1,188
FreeBSD 6.2-RELEASE	18.5%	348
Oracle Solaris 11	4.4%	83
OpenBSD 4.0	3.6%	67
Linux 2.6.32	0.9%	17
Other	9.6%	181

Table 3: Top Operating Systems Detected

Service	Detections	
https	21.9%	486
http-proxy	16.1%	358
jetdirect	11.5%	256
http	11.3%	251
websocket	3.6%	80
Other	35.5%	787

Table 4: Top Services Detected

The next two figures illustrate how quickly SAMPLE responds to vulnerabilities that have been identified. Figure 5 shows how long it has taken SAMPLE to mitigate vulnerabilities of each severity level (for vulnerabilities mitigated since February 4, 2023), while Figure 6 shows the median ages of current active vulnerabilities. Vulnerability age is based on the initial detection date by CyHy.

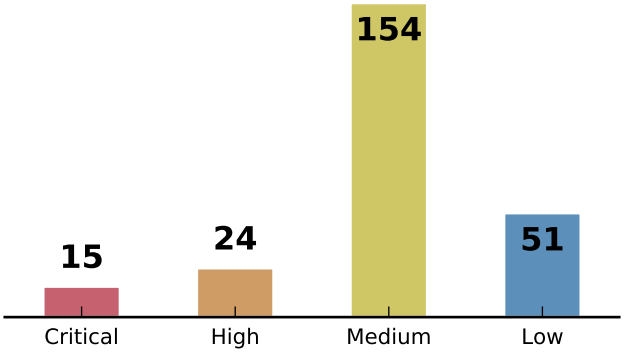


Figure 5: Median Time in Days to Mitigate Vulnerabilities

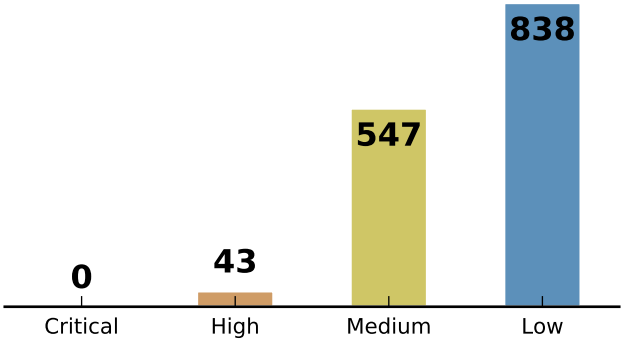


Figure 6: Median Age in Days of Active Vulnerabilities

Figure 7 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.

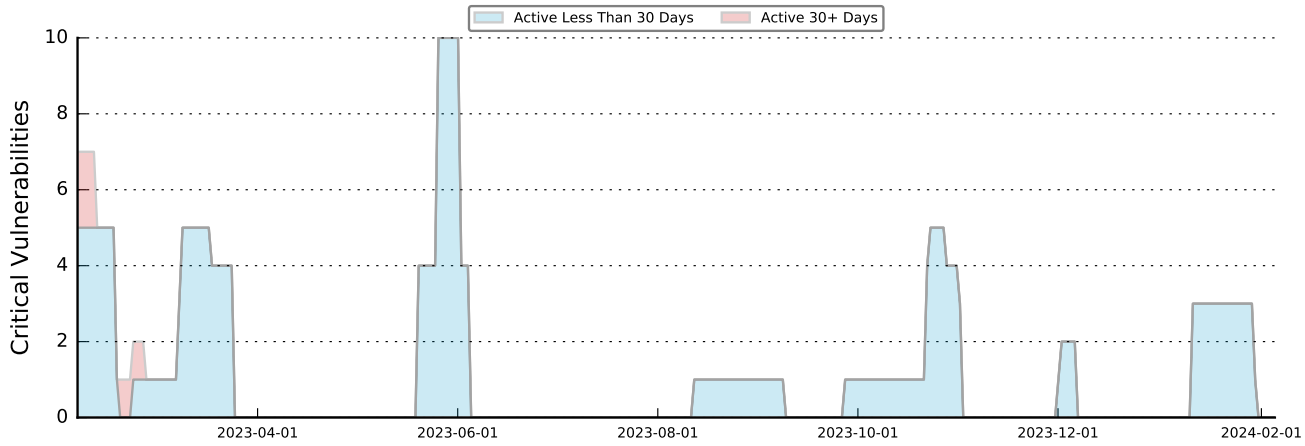


Figure 7: Critical Vulnerability Age Over Time

Figure 8 and Table 5 provide an age breakdown of every currently active critical vulnerability for SAMPLE.

No Critical Vulnerabilities Detected
Figure Omitted

Figure 8: 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	0	0	0	0	0

Table 5: Active Critical Vulnerability Age Summary

7 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	65,630	100%	77	27 (35%)	0	0	49	5	144	16	35	204	273	0	0	546	126
SUB_ORG	628	100%	42	8 (19%)	0	0	12	0	62	0	0	186	31	0	0	138	0
SUB_ORG	2,175	100%	25	1 (4%)	0	0	2	0	37	444	0	232	13	0	0	851	0
SUB_ORG	77,779	100%	93	53 (57%)	0	0	113	5	241	6	7	118	114	0	0	213	139
SUB_ORG	0	0%	0	0 (0%)	0	0	0	0	0	0	0	0	0	0	0	0	0
SUB_ORG	66	100%	7	5 (71%)	0	0	6	9	12	0	0	46	0	0	0	548	1,349
SUB_ORG	73,233	100%	458	131 (29%)	0	1	522	27	1,571	0	39	135	49	0	143	547	813
SUB_ORG	178	100%	18	5 (28%)	0	0	6	2	57	30	55	236	337	0	0	630	506
SUB_ORG	68	100%	13	8 (62%)	0	0	88	0	118	15	15	84	0	0	0	355	0
SUB_ORG	40	100%	16	6 (38%)	0	0	8	0	30	0	0	471	0	0	0	786	0
SUB_ORG	96	100%	73	21 (29%)	0	0	35	3	134	0	5	260	76	0	0	664	852
SUB_ORG	17	100%	1	0 (0%)	0	0	0	0	2	0	0	0	0	0	0	0	0
SUB_ORG	897	100%	4	3 (75%)	0	3	0	0	5	18	0	37	0	0	43	0	0
SAMPLE Total	220,807	100%	827	268 (32%)	0	4	841	51	2,413	15	24	154	51	0	43	547	838

8 Methodology

8.1 Background

CISA conducted a Cyber Hygiene assessment of SAMPLE's Internet-facing networks and hosts from November 6, 2023 at 15:42 UTC through February 4, 2024 at 17:33 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 provided by the Cybersecurity and Infrastructure Security Agency (CISA).

CISA 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 CISA with their public network address information. SAMPLE and CISA agreed on any time restrictions which would be imposed on the scanning activity.

8.2 Process

All Cyber Hygiene scanning activity originates from a dynamic set of Amazon Web Services (AWS) Internet Protocol (IP) addresses in the US East and US West regions. The live list of active addresses can be found at https://rules.ncats.cyber.dhs.gov. The addresses in that list will change based on overall CyHy scan demand.

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 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 CISA 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 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", "High", and "Critical" in addition to the numeric CVSS scores, but these qualitative rankings are simply mapped from the numeric CVSS base scores.

Within this report, qualitative severity rankings are determined primarily by a vulnerability's CVSSv3 base score. If a CVSSv3 base score has not been assigned to a vulnerability, but a CVSSv2 base score has, this report will use the CVSSv2 base score to determine the severity rating with the exception that a base score of 10 will be reported as "Critical." Where the NVD has not provided a CVE severity rating, this report relies on the Nessus scanner's own rating.

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.

9 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.

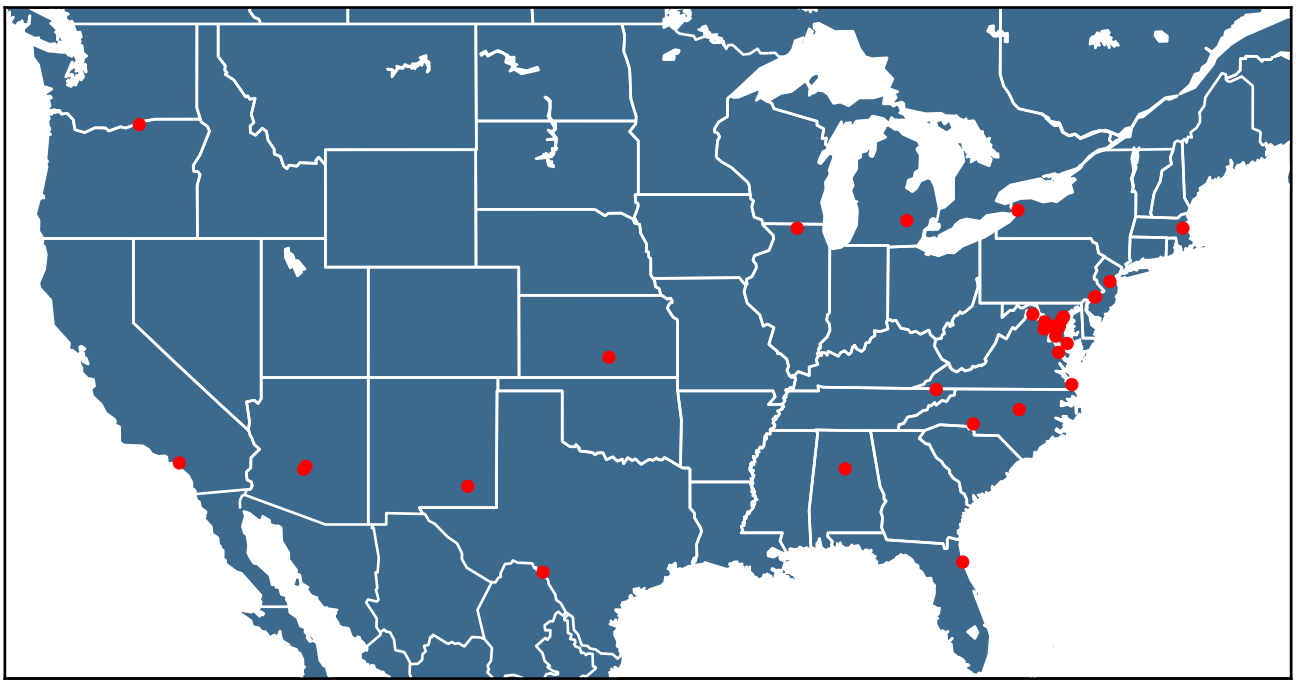


Figure 9: Approximate Host Locations

10 Vulnerability Scan Results

For this period, CyHy detected 896 occurrences of 30 distinct vulnerabilities (0 critical, 4 high, 841 medium, and 51 low). SAMPLE should review the vulnerabilities detected and report any false positives back to CISA so these can be excluded from future reports (see the Frequently Asked Questions section for more about false positives).

The scanning detected 268 vulnerable hosts—242 hosts with one to five vulnerabilities were identified; 2 hosts had between six and nine vulnerabilities; 24 hosts had ten or more vulnerabilities identified.

Severity	Distinct Vulnerabilities		Total Vulnerabilities	
Critical	0%	0	0%	0
High	7%	2	0%	4
Medium	67%	20	94%	841
Low	27%	8	6%	51
Total		30		896

Table 6: Number of Vulnerabilities by Severity Level

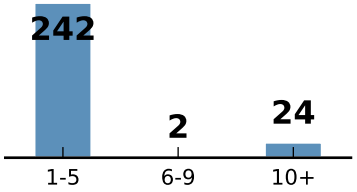


Figure 10: Vulnerability Count per Host

The CVSS scores for all active vulnerabilities can be found in Figure 11.

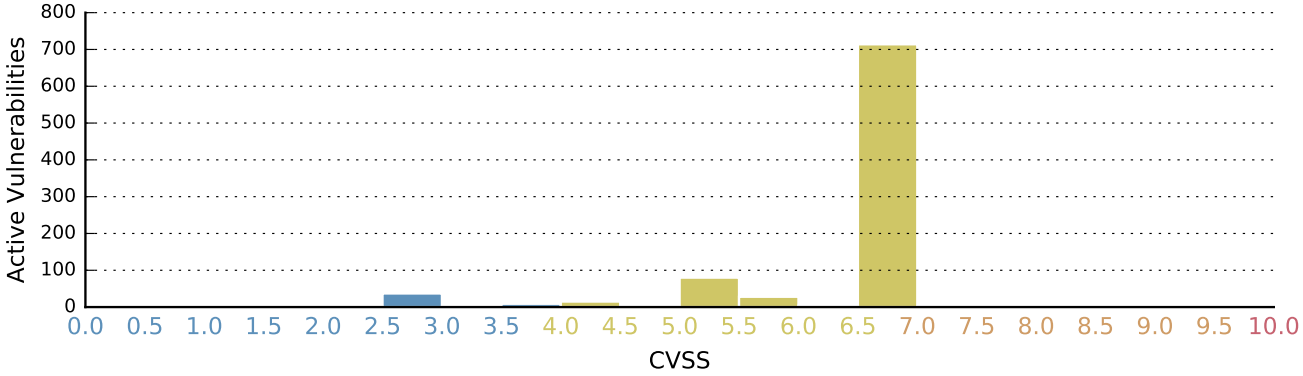


Figure 11: CVSS Histogram for Active Vulnerabilities

The top vulnerabilities according to CVSS score are represented in Table 7.

Vulnerability Name	Severity	Hosts	CVSS Score
Ivanti Connect Secure < 22.6R2 Multiple Vulnerabilities	High	3	7.8
Sun ONE Application Server Upper Case Request JSP Source Disclosure	High	1	7.5
SSL Certificate Cannot Be Trusted	Medium	352	6.5
SSL Self-Signed Certificate	Medium	215	6.5
TLS Version 1.1 Protocol Deprecated	Medium	90	6.5
TLS Version 1.0 Protocol Detection	Medium	49	6.5
HSTS Missing From HTTPS Server (RFC 6797)	Medium	8	6.5
JQuery 1.2 < 3.5.0 Multiple XSS	Medium	4	6.1
SSL Certificate Signed Using Weak Hashing Algorithm	Medium	17	5.9
SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	Medium	11	5.9

Table 7: 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 8 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 9: Risk Rating System.

IP Address	Critical	High	Medium	Low	Total
x.x.51.177	0	0	22	0	22
x.x.59.73	0	0	22	0	22
x.x.49.188	0	0	22	0	22
x.x.51.173	0	0	22	0	22
x.x.51.175	0	0	22	0	22
x.x.51.176	0	0	22	0	22
x.x.51.32	0	0	22	0	22
x.x.59.76	0	0	22	0	22
x.x.59.75	0	0	22	0	22
x.x.59.74	0	0	22	0	22

Table 8: 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 9 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 9: 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).

11 Results Trending

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

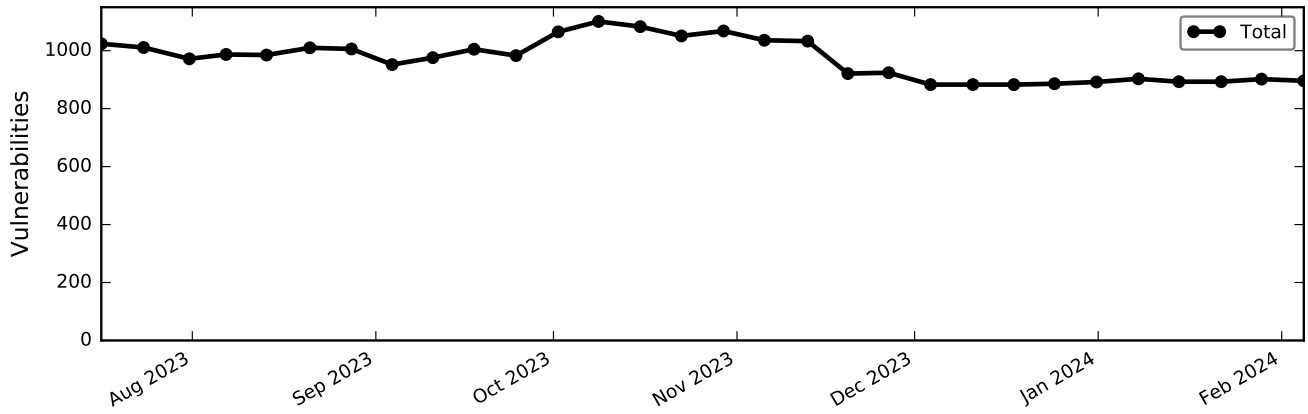


Figure 12: Total Active Vulnerabilities Over Time

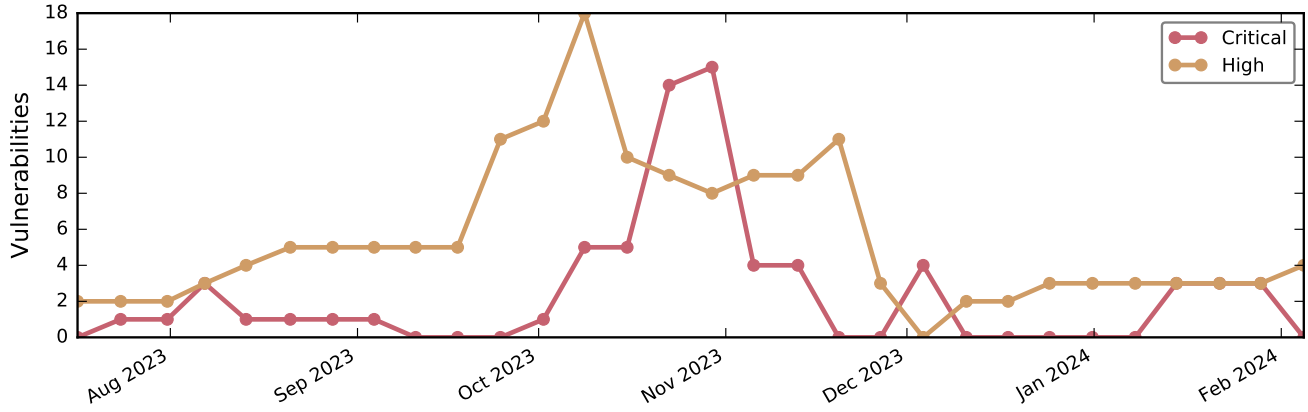


Figure 13: Active Critical and High Vulnerabilities Over Time

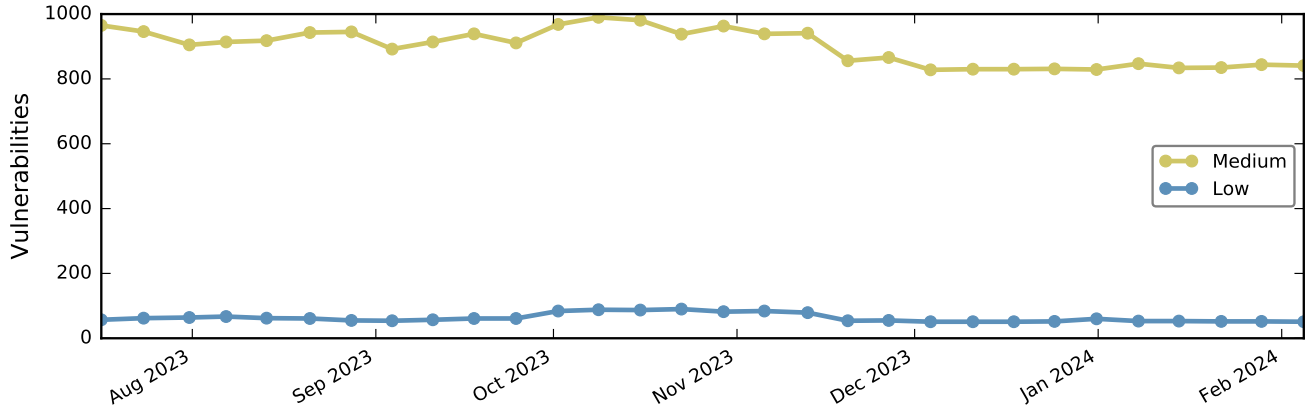


Figure 14: Active Medium and Low Vulnerabilities Over Time

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 15, Figure 16, and Figure 17 respectively.

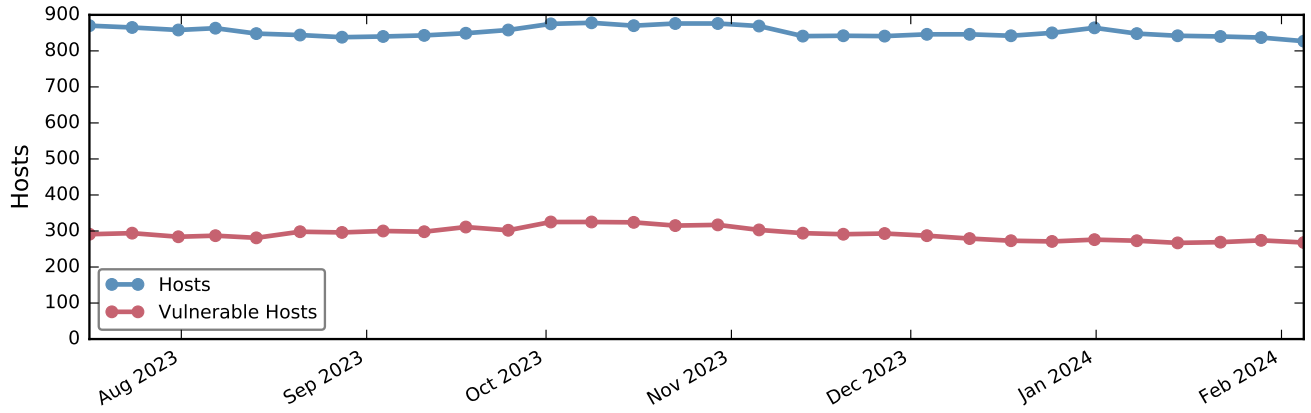


Figure 15: Vulnerable Hosts Over Time

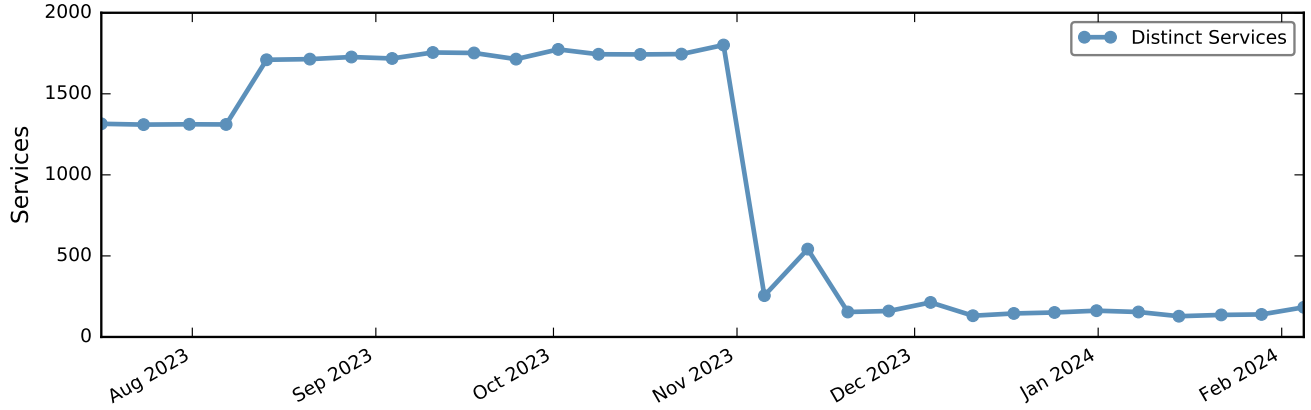


Figure 16: Distinct Services Over Time

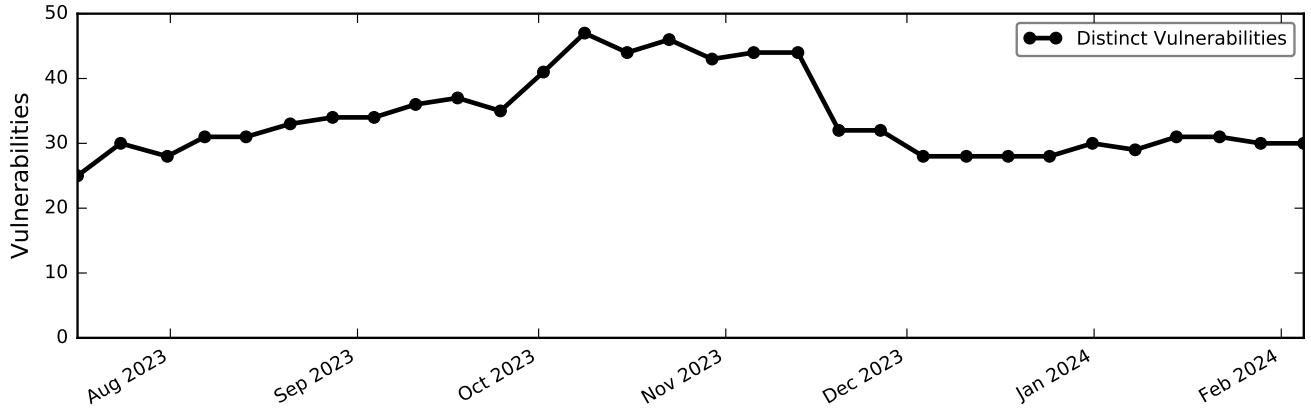


Figure 17: Distinct Vulnerabilities Over Time

	Previous Report	Current Report	% Change
Hosts	837	827	-2.0%
Vulnerable Hosts	274	268	-3.0%
Distinct Services	139	183	31.0%
Distinct Vulnerabilities	30	30	0.0%
Distinct Operating Systems	67	64	-5.0%

Table 10: Comparison with Previous Report

Overall, for all hosts identified, SAMPLE averaged 1.08 vulnerabilities per host. For vulnerable hosts, SAMPLE averaged 3.34 total vulnerabilities per host. By severity, vulnerable hosts averaged 0.0 critical, 0.01 high, 3.14 medium, and 0.19 low vulnerabilities per host.

12 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 CISA at vulnerability@cisa.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
Ivanti Connect Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2023-46805 and CVE-2024-21887)	Critical	3	0	-100.0%
Sun ONE Application Server Upper Case Request JSP Source Disclosure	High	1	1	0.0%
Ivanti Connect Secure < 22.6R2 Multiple Vulnerabilities	High	3	3	0.0%
Web Application Potentially Vulnerable to Clickjacking	Medium	1	3	200.0%
Backup Files Disclosure	Medium	6	7	16.7%
HSTS Missing From HTTPS Server (RFC 6797)	Medium	7	8	14.3%
TLS Version 1.0 Protocol Detection	Medium	48	49	2.1%
HTTP TRACE / TRACK Methods Allowed	Medium	10	10	0.0%
SSH Weak Algorithms Supported	Medium	2	2	0.0%
F5 BIG-IP Cookie Remote Information Disclosure	Medium	2	2	0.0%
Multiple Web Server Encoded Space (%20) Request ASP Source Disclosure	Medium	2	2	0.0%
Nonexistent Page (404) Physical Path Disclosure	Medium	1	1	0.0%
Sun ONE Application Server Upper Case Request JSP Source Disclosure	Medium	1	1	0.0%
Apache Tomcat Default Files	Medium	2	2	0.0%
IIS Detailed Error Information Disclosure	Medium	3	3	0.0%
OpenSSL 1.1.1 < 1.1.1x Vulnerability	Medium	8	8	0.0%
SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	Medium	11	11	0.0%
SSL Certificate Signed Using Weak Hashing Algorithm	Medium	17	17	0.0%
JQuery 1.2 < 3.5.0 Multiple XSS	Medium	4	4	0.0%
TLS Version 1.1 Protocol Deprecated	Medium	90	90	0.0%
SSL Self-Signed Certificate	Medium	216	215	-0.5%
SSL Certificate Cannot Be Trusted	Medium	355	352	-0.8%
SSL Certificate Expiry	Medium	57	54	-5.3%
SSL Anonymous Cipher Suites Supported	Low	2	3	50.0%
Web Server Allows Password Auto-Completion	Low	4	5	25.0%
SSH Server CBC Mode Ciphers Enabled	Low	6	6	0.0%
SSH Weak MAC Algorithms Enabled	Low	7	7	0.0%
SSH Weak Key Exchange Algorithms Enabled	Low	7	7	0.0%
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Low	2	2	0.0%
Web Server HTTP Header Internal IP Disclosure	Low	19	18	-5.3%
Web Server Load Balancer Detection	Low	5	3	-40.0%

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	Ivanti Connect Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2023-46805 and CVE-2024-21887)	Critical	x.x.18.151	443	2024-01-11	2024-01-30 00:01	18
SUB_ORG	Ivanti Connect Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2023-46805 and CVE-2024-21887)	Critical	x.x.18.152	443	2024-01-11	2024-01-30 04:43	18
SUB_ORG	Ivanti Connect Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2023-46805 and CVE-2024-21887)	Critical	x.x.20.200	443	2024-01-11	2024-01-30 00:02	18
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.108.121	8443	2024-01-27	2024-01-31 23:36	4
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.108.75	443	2023-09-16	2024-01-29 17:08	136
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.149	443	2021-10-06	2024-02-02 20:58	849
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.149	8883	2022-08-05	2024-02-02 20:58	547
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.59	443	2024-01-21	2024-01-29 13:25	8
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.52.116	4502	2024-01-26	2024-01-30 18:42	4
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.52.117	4502	2024-01-26	2024-01-30 07:36	4
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.59.77	1805	2022-08-05	2024-02-01 01:07	545
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.60.151	4502	2024-01-26	2024-01-30 15:23	4
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.60.152	4502	2024-01-26	2024-01-30 15:41	4
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.183	443	2023-12-19	2024-02-03 02:54	46
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.87.145	443	2016-07-21	2024-01-29 11:39	2748
SUB_ORG	SSL Certificate Expiry	Medium	x.x.52.116	4502	2024-01-26	2024-01-30 18:42	4
SUB_ORG	SSL Certificate Expiry	Medium	x.x.52.117	4502	2024-01-26	2024-01-30 07:36	4
SUB_ORG	SSL Certificate Expiry	Medium	x.x.60.151	4502	2024-01-26	2024-01-30 15:23	4
SUB_ORG	SSL Certificate Expiry	Medium	x.x.60.152	4502	2024-01-26	2024-01-30 15:41	4
SUB_ORG	SSL Certificate Expiry	Medium	x.x.60.34	443	2024-01-26	2024-01-30 13:35	4
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.108.121	8443	2024-01-27	2024-01-31 23:36	4
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.59.77	1805	2022-08-05	2024-02-01 01:07	545
SUB_ORG	TLS Version 1.1 Protocol Deprecated	Medium	x.x.108.121	8443	2024-01-27	2024-01-31 23:36	4
SUB_ORG	Web Server Allows Password Auto-Completion	Low	x.x.108.75	443	2023-09-16	2024-01-29 17:08	136
SUB_ORG	Web Server HTTP Header Internal IP Disclosure	Low	x.x.50.149	443	2021-10-06	2024-02-02 20:58	849
SUB_ORG	Web Server HTTP Header Internal IP Disclosure	Low	x.x.52.213	443	2024-01-24	2024-02-01 13:17	8
SUB_ORG	Web Server HTTP Header Internal IP Disclosure	Low	x.x.60.227	443	2024-01-24	2024-02-01 15:04	8
SUB_ORG	Web Server Load Balancer Detection	Low	x.x.50.53	443	2023-05-27	2024-01-29 22:43	247

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Mitigation Detected (UTC)	Days To Mitigate
SUB_ORG	Web Server Load Balancer Detection	Low	x.x.89.152	443	2022-12-16	2024-01-29 19:33	409

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 vulnerability.

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)
SUB_ORG	HSTS Missing From HTTPS Server (RFC 6797)	Medium	x.x.80.167	443	2024-02-04 07:11	2024-02-04 07:11
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.253	443	2024-02-03 12:30	2024-02-03 12:30
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.69	443	2024-02-04 03:53	2024-02-04 03:53
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.58.55	443	2024-01-31 07:40	2024-02-04 17:05

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 vulnerability.

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	Age Days
SUB_ORG	Backup Files Disclosure	Medium	x.x.51.172	443	2023-10-20 14:36	2024-02-02 19:12	105
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.108.74	443	2023-09-18 16:04	2024-02-03 13:19	137
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.108.76	443	2023-09-19 11:21	2024-02-04 04:10	137
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.49.143	443	2023-10-03 11:32	2024-02-03 03:32	122
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.137	443	2021-10-07 00:18	2024-02-03 13:23	849
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.59.77	8443	2021-10-06 16:20	2024-02-01 01:47	847
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.30	443	2018-06-29 08:27	2024-02-03 17:22	2045
SUB_ORG	SSL Certificate Expiry	Medium	x.x.49.143	443	2023-10-03 11:32	2024-02-03 03:32	122
SUB_ORG	SSL Certificate Expiry	Medium	x.x.80.30	443	2022-11-29 16:11	2024-02-03 17:22	431
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.59.77	8443	2021-10-06 16:20	2024-02-01 01:47	847
SUB_ORG	TLS Version 1.0 Protocol Detection	Medium	x.x.80.46	443	2021-10-06 23:13	2024-02-03 02:33	849
SUB_ORG	TLS Version 1.1 Protocol Deprecated	Medium	x.x.80.46	443	2022-04-07 19:37	2024-02-03 02:33	666
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.49.220	443	2023-11-24 05:46	2024-02-02 23:01	70
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.51.144	443	2023-08-16 07:24	2024-02-04 07:15	171

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	Age Days
SUB_ORG	SSL Anonymous Cipher Suites Supported	Low	x.x.80.46	443	2021-10-06 23:13	2024-02-03 02:33	849
SUB_ORG	Web Server Allows Password Auto-Completion	Low	x.x.108.74	443	2023-09-18 16:04	2024-02-03 13:19	137
SUB_ORG	Web Server Allows Password Auto-Completion	Low	x.x.108.76	443	2023-09-19 11:21	2024-02-04 04:10	137
SUB_ORG	Web Server HTTP Header Internal IP Disclosure	Low	x.x.50.137	443	2021-10-07 00:18	2024-02-03 13:23	849
SUB_ORG	Web Server HTTP Header Internal IP Disclosure	Low	x.x.50.152	443	2021-10-06 16:42	2024-02-04 14:52	850

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	Ivanti Connect Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2023-46805 and CVE-2024-21887)	Critical	x.x.18.152	443	2024-01-11 21:23	2024-01-29 11:27	17
SUB_ORG	Ivanti Connect Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2023-46805 and CVE-2024-21887)	Critical	x.x.18.151	443	2024-01-11 21:46	2024-01-29 10:00	17
SUB_ORG	Ivanti Connect Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2023-46805 and CVE-2024-21887)	Critical	x.x.20.200	443	2024-01-11 23:05	2024-01-29 10:41	17
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.149	443	2021-10-06 19:20	2024-01-29 19:44	845
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.149	8883	2022-08-05 06:33	2024-01-29 19:44	542
SUB_ORG	SGDynamo sgdynamo.exe HTNAME Parameter Path Disclosure	Medium	x.x.50.49	443	2023-06-14 06:10	2024-01-29 21:46	229
SUB_ORG	Backup Files Disclosure	Medium	x.x.88.138	443	2023-09-08 02:12	2024-01-29 18:37	143
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.183	443	2023-12-19 13:36	2024-01-29 19:46	41
SUB_ORG	Web Server HTTP Header Internal IP Disclosure	Low	x.x.50.149	443	2021-10-06 19:20	2024-01-29 19:44	845

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
Ivanti Connect Secure < 22.6R2 Multiple Vulnerabilities	High	7.8	Upgrade to Ivanti Secure Desktop Client 22.6R2 or later.

3 Affected Host(s): x.x.18.151, x.x.18.152, x.x.20.200
Initial Detection: 2023-12-22 21:01 UTC
Latest Detection: 2024-02-04 15:30 UTC
Description: The Ivanti Connect Secure installed on the remote host is prior to 22.6R2. It is, therefore, affected by multiple vulnerabilities.

- A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance. (CVE-2023-39340)

- A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker impersonating an administrator may craft a specific web request which may lead to remote code execution. (CVE-2023-41719)

- A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where a local attacker with access to an Ivanti Connect Secure (ICS) appliance can escalate their privileges by exploiting a vulnerable installed application. This vulnerability allows the attacker to gain elevated execution privileges on the affected system. (CVE-2023-41720)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Sun ONE Application Server Upper Case Request JSP Source Disclosure	High	7.5	Upgrade to Sun ONE Application Server 7.0 Update Release 1.

1 Affected Host(s): x.x.58.57
Initial Detection: 2023-09-14 18:36 UTC
Latest Detection: 2024-02-04 12:07 UTC
Description: It is possible to make the remote web server disclose the source code of its JSP pages by requesting the pages with a different case (ie:
filename.JSP instead of filename.jsp).

An attacker may use this flaw to get the source code of your CGIs and possibly obtain passwords and other relevant information about this host.

Vulnerability	Severity	CVSS	Solution
HSTS Missing From HTTPS Server (RFC 6797)	Medium	6.5	Configure the remote web server to use HSTS.

7 Affected Host(s): x.x.28.66, x.x.80.163, x.x.80.164, x.x.80.167, x.x.82.145, x.x.92.46, x.x.92.50

Initial Detection: 2021-03-14 20:11 UTC

Latest Detection: 2024-02-04 07:11 UTC

Description: The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

Vulnerability	Severity	CVSS	Solution
SSL Certificate Cannot Be Trusted	Medium	6.5	Purchase or generate a proper SSL certificate for this service.

180 Affected Host(s): x.x.108.72, x.x.108.74, x.x.108.76, x.x.108.77, x.x.113.2, x.x.121.186, x.x.125.169, x.x.135.90, x.x.187.130, x.x.48.146, x.x.49.103, x.x.49.111, x.x.49.127, x.x.49.128, x.x.49.13, x.x.49.143, x.x.49.144, x.x.49.146, x.x.49.188, x.x.49.195, x.x.49.196, x.x.49.218, x.x.49.247, x.x.49.248, x.x.49.85, x.x.49.86, x.x.50.110, x.x.50.111, x.x.50.137, x.x.50.152, x.x.50.155, x.x.50.158, x.x.50.16, x.x.50.17, x.x.50.18, x.x.50.188, x.x.50.21, x.x.50.218, x.x.50.24, x.x.50.252, x.x.50.253, x.x.50.32, x.x.51.1, x.x.51.13, x.x.51.134, x.x.51.135, x.x.51.138, x.x.51.139, x.x.51.14, x.x.51.143, x.x.51.155, x.x.51.160, x.x.51.162, x.x.51.173, x.x.51.175, x.x.51.176, x.x.51.177, x.x.51.184, x.x.51.221, x.x.51.236, x.x.51.24, x.x.51.31, x.x.51.32, x.x.51.38, x.x.51.39, x.x.51.40, x.x.51.42, x.x.51.55, x.x.51.69, x.x.52.125, x.x.52.144, x.x.52.145, x.x.52.193, x.x.52.194, x.x.52.214, x.x.52.218, x.x.57.105, x.x.57.106, x.x.57.108, x.x.57.122, x.x.57.123, x.x.57.13, x.x.57.138, x.x.57.139, x.x.57.141, x.x.57.188, x.x.57.221, x.x.57.222, x.x.57.225, x.x.57.235, x.x.57.74, x.x.57.89, x.x.57.90, x.x.58.101, x.x.58.102, x.x.58.11, x.x.58.143, x.x.58.146, x.x.58.15, x.x.58.179, x.x.58.202, x.x.58.203, x.x.58.21, x.x.58.225, x.x.58.232, x.x.58.240, x.x.58.241, x.x.58.242, x.x.58.248, x.x.58.249, x.x.58.25, x.x.58.250, x.x.58.251, x.x.58.55, x.x.58.6, x.x.58.7, x.x.58.72, x.x.59.12, x.x.59.13, x.x.59.15, x.x.59.32, x.x.59.38, x.x.59.43, x.x.59.54, x.x.59.61, x.x.59.63, x.x.59.68, x.x.59.69, x.x.59.73, x.x.59.74, x.x.59.75, x.x.59.76, x.x.59.77, x.x.59.79, x.x.59.81, x.x.59.88, x.x.60.12, x.x.60.128, x.x.60.129, x.x.60.13, x.x.60.138, x.x.60.157, x.x.60.158, x.x.60.161, x.x.60.162, x.x.60.163, x.x.60.167, x.x.60.168, x.x.60.193, x.x.60.198, x.x.60.199, x.x.60.207, x.x.60.224, x.x.60.225, x.x.60.228, x.x.60.230, x.x.60.231, x.x.60.232, x.x.60.34, x.x.80.186, x.x.80.234, x.x.80.30, x.x.80.33, x.x.80.57, x.x.84.145, x.x.85.159, x.x.85.160, x.x.85.166, x.x.87.21, x.x.87.3, x.x.87.4, x.x.89.129, x.x.91.187, x.x.91.188, x.x.92.152, x.x.92.171, x.x.92.249, x.x.93.2, x.x.95.15, x.x.95.32

Initial Detection: 2016-09-06 09:37 UTC

Latest Detection: 2024-02-04 17:29 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.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Vulnerability	Severity	CVSS	Solution
SSL Self-Signed Certificate	Medium	6.5	Purchase or generate a proper SSL certificate for this service.

49 Affected Host(s): x.x.113.2, x.x.121.186, x.x.125.169, x.x.135.90, x.x.187.130, x.x.48.146, x.x.49.188, x.x.49.247, x.x.49.248, x.x.50.110, x.x.50.111, x.x.50.32, x.x.51.138, x.x.51.155, x.x.51.173, x.x.51.175, x.x.51.176, x.x.51.177, x.x.51.31, x.x.51.32, x.x.57.188, x.x.57.221, x.x.57.222, x.x.57.225, x.x.57.74, x.x.58.101, x.x.58.102, x.x.58.240, x.x.58.241, x.x.58.242, x.x.58.25, x.x.59.38, x.x.59.54, x.x.59.73, x.x.59.74, x.x.59.75, x.x.59.76, x.x.59.77, x.x.60.230, x.x.60.231, x.x.80.234, x.x.80.57, x.x.84.145, x.x.87.3, x.x.87.4, x.x.89.129, x.x.92.152, x.x.92.249, x.x.93.2

Initial Detection: 2020-04-05 17:21 UTC

Latest Detection: 2024-02-04 16:32 UTC

Description: The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

TLS Version 1.0 Protocol Detection	Medium	6.5	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

17 Affected Host(s): x.x.113.2, x.x.187.130, x.x.49.170, x.x.51.44, x.x.52.128, x.x.58.232, x.x.58.249, x.x.58.7, x.x.59.68, x.x.59.69, x.x.60.162, x.x.60.163, x.x.80.48, x.x.80.57, x.x.92.65, x.x.93.2, x.x.95.108

Initial Detection: 2020-04-02 00:42 UTC

Latest Detection: 2024-02-04 17:06 UTC

Description: The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that arenâ€™t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Vulnerability	Severity	CVSS	Solution
TLS Version 1.0 Protocol Detection	Medium	6.5	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

28 Affected Host(s): x.x.121.186, x.x.125.169, x.x.135.90, x.x.48.146, x.x.49.112, x.x.49.168, x.x.49.193, x.x.50.16, x.x.50.17, x.x.50.18, x.x.51.136, x.x.51.139, x.x.51.14, x.x.51.77, x.x.52.125, x.x.57.168, x.x.57.178, x.x.57.235, x.x.58.254, x.x.58.6, x.x.59.33, x.x.59.81, x.x.60.161, x.x.80.46, x.x.85.166, x.x.92.249, x.x.92.61, x.x.95.15
Initial Detection: 2020-04-02 05:14 UTC
Latest Detection: 2024-02-04 16:23 UTC
Description: The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

TLS Version 1.1 Protocol Deprecated	Medium	6.5	Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

76 Affected Host(s): x.x.113.2, x.x.121.186, x.x.125.169, x.x.135.90, x.x.187.130, x.x.48.146, x.x.49.168, x.x.49.170, x.x.49.174, x.x.49.193, x.x.49.195, x.x.49.196, x.x.49.233, x.x.50.16, x.x.50.17, x.x.50.18, x.x.50.253, x.x.51.134, x.x.51.135, x.x.51.136, x.x.51.139, x.x.51.14, x.x.51.143, x.x.51.144, x.x.51.172, x.x.51.208, x.x.51.229, x.x.51.230, x.x.51.38, x.x.51.39, x.x.51.40, x.x.51.42, x.x.51.44, x.x.51.69, x.x.51.77, x.x.52.125, x.x.57.168, x.x.57.178, x.x.57.238, x.x.58.203, x.x.58.232, x.x.58.248, x.x.58.249, x.x.58.250, x.x.58.251, x.x.58.254, x.x.58.6, x.x.58.7, x.x.59.12, x.x.59.127, x.x.59.13, x.x.59.32, x.x.59.33, x.x.59.43, x.x.59.68, x.x.59.69, x.x.59.72, x.x.59.79, x.x.59.81, x.x.60.161, x.x.60.162, x.x.60.163, x.x.60.198, x.x.80.46, x.x.80.48, x.x.82.145, x.x.88.161, x.x.91.209, x.x.91.248, x.x.91.250, x.x.91.251, x.x.92.249, x.x.92.61, x.x.92.65, x.x.93.2, x.x.95.108
Initial Detection: 2022-04-05 02:58 UTC
Latest Detection: 2024-02-04 17:06 UTC
Description: The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

Vulnerability	Severity	CVSS	Solution
JQuery 1.2 < 3.5.0 Multiple XSS	Medium	6.1	Upgrade to JQuery version 3.5.0 or later.
	4 Affected Host(s): x.x.109.211, x.x.50.155, x.x.58.143, x.x.83.87 *Initial Detection:* 2021-10-07 01:58 UTC *Latest Detection:* 2024-02-04 02:28 UTC *Description:* According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities. Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release.		
SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	Medium	5.9	Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.
	11 Affected Host(s): x.x.113.2, x.x.121.186, x.x.125.169, x.x.135.90, x.x.187.130, x.x.48.146, x.x.49.182, x.x.51.235, x.x.57.182, x.x.92.249, x.x.93.2 *Initial Detection:* 2023-12-28 03:12 UTC *Latest Detection:* 2024-02-04 14:44 UTC *Description:* The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security. Note that this plugin only checks for remote SSH servers that support either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC and do not support the strict key exchange countermeasures. It does not check for vulnerable software versions.		
SSL Certificate Signed Using Weak Hashing Algorithm	Medium	5.9	Contact the Certificate Authority to have the SSL certificate reissued.
	9 Affected Host(s): x.x.113.2, x.x.121.186, x.x.125.169, x.x.135.90, x.x.187.130, x.x.48.146, x.x.80.161, x.x.92.249, x.x.93.2 *Initial Detection:* 2022-06-22 01:24 UTC *Latest Detection:* 2024-02-04 09:36 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
Apache Tomcat Default Files	Medium	5.3	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.51.135, x.x.59.13 *Initial Detection:* 2021-10-06 04:01 UTC *Latest Detection:* 2024-02-02 21:12 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.		
IIS Detailed Error Information Disclosure	Medium	5.3	Configure the IIS server to deliver custom rather than detailed error messages.
	3 Affected Host(s): x.x.50.47, x.x.58.40, x.x.58.42 *Initial Detection:* 2023-06-24 13:24 UTC *Latest Detection:* 2024-02-04 16:34 UTC *Description:* The remote Microsoft IIS web server is improperly configured to deliver detailed error messages. These detailed error messages may contain confidential diagnostic information, such as the file system paths to hosted content and logon information.		
OpenSSL 1.1.1 < 1.1.1x Vulnerability	Medium	5.3	Upgrade to OpenSSL version 1.1.1x or later.
	8 Affected Host(s): x.x.50.110, x.x.50.111, x.x.52.176, x.x.52.177, x.x.58.101, x.x.58.102, x.x.60.195, x.x.60.196 *Initial Detection:* 2023-11-08 00:17 UTC *Latest Detection:* 2024-02-04 04:34 UTC *Description:* The version of OpenSSL installed on the remote host is prior to 1.1.1x. It is, therefore, affected by a vulnerability as referenced in the 1.1.1x advisory. - Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the -pubcheck option, as well as the OpenSSL genpkey command line application. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. (CVE-2023-5678) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.		

Vulnerability	Severity	CVSS	Solution
SSL Certificate Expiry	Medium	5.3	Purchase or generate a new SSL certificate to replace the existing one.
	43 Affected Host(s): x.x.113.2, x.x.121.186, x.x.125.169, x.x.135.90, x.x.187.130, x.x.48.146, x.x.49.143, x.x.49.144, x.x.51.13, x.x.51.134, x.x.51.135, x.x.51.143, x.x.51.38, x.x.51.39, x.x.51.40, x.x.51.42, x.x.52.125, x.x.57.108, x.x.57.138, x.x.57.139, x.x.57.74, x.x.58.203, x.x.58.21, x.x.58.248, x.x.58.249, x.x.58.250, x.x.58.251, x.x.58.72, x.x.59.12, x.x.59.13, x.x.59.15, x.x.59.43, x.x.59.68, x.x.59.69, x.x.60.138, x.x.60.161, x.x.60.162, x.x.60.163, x.x.80.30, x.x.80.57, x.x.92.171, x.x.92.249, x.x.93.2 *Initial Detection:* 2021-10-06 06:33 UTC *Latest Detection:* 2024-02-04 17:06 UTC *Description:* This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.		
Backup Files Disclosure	Medium	5.0	Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.
	7 Affected Host(s): x.x.51.172, x.x.57.105, x.x.57.129, x.x.57.140, x.x.57.141, x.x.59.72, x.x.85.185 *Initial Detection:* 2022-05-04 17:21 UTC *Latest Detection:* 2024-02-04 16:41 UTC *Description:* By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.		
F5 BIG-IP Cookie Remote Information Disclosure	Medium	5.0	Contact the vendor for a fix.
	2 Affected Host(s): x.x.80.172, x.x.83.87 *Initial Detection:* 2023-09-11 10:27 UTC *Latest Detection:* 2024-02-04 03:44 UTC *Description:* The remote host appears to be an F5 BIG-IP load balancer. The load balancer encodes the IP address of the actual web server that it is acting on behalf of within a cookie. Additionally, information after 'BIGipServer' is configured by the user and may be the logical name of the device. These values may disclose sensitive information, such as internal IP addresses and names.		
Multiple Web Server Encoded Space (%20) Request ASP Source Disclosure	Medium	5.0	There is no known solution at this time.
	2 Affected Host(s): x.x.50.68, x.x.58.57 *Initial Detection:* 2023-09-08 01:14 UTC *Latest Detection:* 2024-02-04 12:07 UTC *Description:* It appears possible to get the source code of the remote ASP scripts by appending a '%20' to the request. ASP source code usually contains sensitive information such as logins and passwords. This has been reported in Simple HTTPD (shttpd), Mono XSP for ASP.NET and vWebServer. This type of request may affect other web servers as well.		

Vulnerability	Severity	CVSS	Solution
Nonexistent Page (404) Physical Path Disclosure	Medium	5.0	Upgrade the web server to the latest version. Alternatively, reconfigure the web server to disable debug reporting.
	1 Affected Host(s): x.x.50.49 *Initial Detection:* 2023-06-26 14:26 UTC *Latest Detection:* 2024-02-03 02:56 UTC *Description:* The remote web server reveals the physical path of the webroot when a nonexistent page is requested. While printing errors to the output is useful for debugging applications, this feature should be disabled on production servers.		
Sun ONE Application Server Upper Case Request JSP Source Disclosure	Medium	5.0	Upgrade to Sun ONE Application Server 7.0 Update Release 1.
	1 Affected Host(s): x.x.50.68 *Initial Detection:* 2023-09-08 01:14 UTC *Latest Detection:* 2024-02-01 03:22 UTC *Description:* It is possible to make the remote web server disclose the source code of its JSP pages by requesting the pages with a different case (ie: filename.JSP instead of filename.jsp). An attacker may use this flaw to get the source code of your CGIs and possibly obtain passwords and other relevant information about this host.		
HTTP TRACE / TRACK Methods Allowed	Medium	4.3	Disable these HTTP methods. Refer to the plugin output for more information.
	10 Affected Host(s): x.x.109.141, x.x.109.142, x.x.109.143, x.x.109.181, x.x.109.205, x.x.52.176, x.x.52.177, x.x.60.195, x.x.60.196, x.x.60.41 *Initial Detection:* 2017-08-30 17:29 UTC *Latest Detection:* 2024-02-04 04:17 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.		
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.49.182, x.x.57.182 *Initial Detection:* 2021-10-06 13:13 UTC *Latest Detection:* 2024-02-04 14:44 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.		

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.

3 Affected Host(s): x.x.49.220, x.x.51.144, x.x.59.44
Initial Detection: 2023-08-16 07:24 UTC
Latest Detection: 2024-02-04 07:15 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.

Vulnerability	Severity	CVSS	Solution
SSH Weak Key Exchange Algorithms Enabled	Low	3.7	Contact the vendor or consult product documentation to disable the weak algorithms.

7 Affected Host(s): x.x.131.161, x.x.207.145, x.x.58.228, x.x.58.229, x.x.6.41, x.x.60.201, x.x.83.74
Initial Detection: 2021-10-14 16:24 UTC
Latest Detection: 2024-02-03 03:36 UTC
Description: The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Low	3.7	Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

2 Affected Host(s): x.x.50.17, x.x.58.7
Initial Detection: 2021-11-12 17:26 UTC
Latest Detection: 2024-02-04 04:04 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.

Vulnerability	Severity	CVSS	Solution
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.
	6 Affected Host(s): x.x.49.182, x.x.57.182, x.x.58.228, x.x.58.229, x.x.6.41, x.x.83.74 *Initial Detection:* 2016-04-26 15:35 UTC *Latest Detection:* 2024-02-04 14:44 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.
	7 Affected Host(s): x.x.131.161, x.x.207.145, x.x.58.228, x.x.58.229, x.x.6.41, x.x.60.201, x.x.83.74 *Initial Detection:* 2020-02-05 17:41 UTC *Latest Detection:* 2024-02-03 03:36 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.		
SSL Anonymous Cipher Suites Supported	Low	2.6	Reconfigure the affected application if possible to avoid use of weak ciphers.
	3 Affected Host(s): x.x.51.77, x.x.80.46, x.x.80.48 *Initial Detection:* 2021-10-05 21:24 UTC *Latest Detection:* 2024-02-04 00:11 UTC *Description:* The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack. Note: This is considerably easier to exploit if the attacker is on the same physical network.		
Web Server HTTP Header Internal IP Disclosure	Low	2.6	Apply configuration suggested by vendor.
	18 Affected Host(s): x.x.109.146, x.x.49.111, x.x.49.112, x.x.49.134, x.x.49.135, x.x.49.136, x.x.50.137, x.x.50.152, x.x.52.182, x.x.57.105, x.x.57.106, x.x.57.107, x.x.57.129, x.x.57.130, x.x.57.131, x.x.58.66, x.x.82.145, x.x.87.227 *Initial Detection:* 2019-03-31 17:57 UTC *Latest Detection:* 2024-02-04 17:28 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.		

Vulnerability	Severity	CVSS	Solution
Web Server Load Balancer Detection	Low	2.6	Update the web configuration to hide information disclosure.
	3 Affected Host(s): x.x.52.182, x.x.82.145, x.x.87.227 *Initial Detection:* 2020-01-24 05:52 UTC *Latest Detection:* 2024-02-03 03:54 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 Allows Password Auto-Completion	Low	0.0	Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.
	5 Affected Host(s): x.x.108.72, x.x.108.74, x.x.108.76, x.x.108.77, x.x.64.167 *Initial Detection:* 2023-07-22 11:12 UTC *Latest Detection:* 2024-02-04 08:09 UTC *Description:* The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'. While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.		

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.18.151	443	Ivanti Connect Secure < 22.6R2 Multiple Vulnerabilities	High	42	Upgrade to Ivanti Secure Desktop Client 22.6R2 or later.
SUB_ORG	x.x.18.152	443	Ivanti Connect Secure < 22.6R2 Multiple Vulnerabilities	High	43	Upgrade to Ivanti Secure Desktop Client 22.6R2 or later.
SUB_ORG	x.x.20.200	443	Ivanti Connect Secure < 22.6R2 Multiple Vulnerabilities	High	42	Upgrade to Ivanti Secure Desktop Client 22.6R2 or later.
SUB_ORG	x.x.58.57	443	Sun ONE Application Server Upper Case Request JSP Source Disclosure	High	142	Upgrade to Sun ONE Application Server 7.0 Update Release 1.

Appendix E False Positive Findings

This section lists findings that SAMPLE asserted to CISA to be false positives (i.e., data that incorrectly indicates a vulnerability is present). If SAMPLE would like to report findings for false positive consideration, please complete the False Positive Assertion Form included in Appendix G: Attachments. Unless CISA determines the submission is insufficient, CISA 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 CISA. When a finding's false positive status expires, the finding will be removed from this section. If the finding is then re-detected, CISA recommends SAMPLE review its status.

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 (UTC)	Latest Detection (UTC)	False Positive Effective	False Positive Expiration
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.43	443	2021-10-07 04:16	2024-01-14 05:08	2023-10-20	2024-02-20
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.58.252	443	2022-02-09 06:14	2024-01-13 23:16	2023-10-20	2024-02-20
SUB_ORG	TLS Version 1.1 Protocol Deprecated	Medium	x.x.51.43	443	2022-04-07 03:04	2024-01-14 05:08	2023-11-27	2024-02-20
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.58.252	443	2023-01-29 08:31	2024-01-13 23:16	2023-03-03	2024-03-02
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.83.72	443	2023-01-30 09:56	2023-11-25 20:32	2023-03-03	2024-03-02
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.51.43	443	2023-01-30 10:25	2024-01-14 05:08	2023-03-03	2024-03-02
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.160.139	443	2023-02-14 21:41	2024-02-04 04:01	2023-06-01	2024-03-04

E.2 All False Positive Findings

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	False Positive Effective	False Positive Expiration
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.43	443	2021-10-07 04:16	2024-01-14 05:08	2023-10-20	2024-02-20
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.58.252	443	2022-02-09 06:14	2024-01-13 23:16	2023-10-20	2024-02-20
SUB_ORG	TLS Version 1.1 Protocol Deprecated	Medium	x.x.51.43	443	2022-04-07 03:04	2024-01-14 05:08	2023-11-27	2024-02-20
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.58.252	443	2023-01-29 08:31	2024-01-13 23:16	2023-03-03	2024-03-02
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.83.72	443	2023-01-30 09:56	2023-11-25 20:32	2023-03-03	2024-03-02
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.51.43	443	2023-01-30 10:25	2024-01-14 05:08	2023-03-03	2024-03-02
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.160.139	443	2023-02-14 21:41	2024-02-04 04:01	2023-06-01	2024-03-04
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.162	443	2023-02-21 21:00	2024-02-04 03:58	2023-06-28	2024-03-18
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.150	443	2016-09-02 14:25	2024-02-04 04:22	2023-04-07	2024-04-06

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	False Positive Effective	False Positive Expiration
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.150	443	2016-09-02 14:25	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.150	10443	2019-03-28 15:16	2024-02-04 04:22	2023-10-09	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.150	10443	2019-03-28 15:16	2024-02-04 04:22	2023-10-09	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.137	443	2021-10-06 05:03	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.137	10443	2021-10-06 05:03	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.137	443	2021-10-06 05:03	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.137	10443	2021-10-06 05:03	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.52	443	2021-10-07 05:03	2024-02-04 17:13	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.150	643	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.150	643	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.150	1443	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.150	1443	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.150	7443	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.150	7443	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.150	6443	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.150	6443	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.150	4443	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.150	4443	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.137	7443	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.137	7443	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.137	1443	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.137	1443	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.137	6443	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.137	6443	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.137	643	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.137	643	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.137	4443	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.137	4443	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.18.152	443	2020-04-10 11:14	2024-02-04 15:30	2023-07-05	2024-04-10
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.18.152	443	2020-04-10 11:14	2024-02-04 15:30	2023-07-05	2024-04-10
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.18.151	443	2020-04-10 11:18	2024-02-04 11:09	2023-07-05	2024-04-10
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.18.151	443	2020-04-10 11:18	2024-02-04 11:09	2023-07-05	2024-04-10
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.20.200	443	2020-04-10 11:22	2024-02-04 11:15	2023-07-05	2024-04-10
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.20.200	443	2020-04-10 11:22	2024-02-04 11:15	2023-07-05	2024-04-10
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.0	443	2021-10-05 23:32	2024-02-02 17:46	2023-09-27	2024-05-17
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.58.224	443	2021-10-06 18:11	2024-02-04 03:27	2023-09-27	2024-05-17
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.11	443	2021-10-06 10:02	2024-02-03 23:40	2023-09-27	2024-05-19
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.58.20	443	2021-10-06 20:42	2024-02-04 04:31	2023-09-20	2024-05-19
SUB_ORG	SSL Certificate Expiry	Medium	x.x.51.11	443	2023-05-11 22:46	2024-02-03 23:40	2023-09-27	2024-05-19

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	False Positive Effective	False Positive Expiration
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.41	443	2023-06-07 17:04	2024-02-04 04:37	2023-07-14	2024-06-08
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.9.44	443	2021-07-09 15:34	2024-01-25 03:11	2023-06-15	2024-06-14
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.9.44	443	2021-07-09 15:34	2024-01-25 03:11	2023-06-15	2024-06-14
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.203.203	443	2021-07-09 15:34	2024-02-02 17:37	2023-07-10	2024-06-20
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.161	443	2022-06-08 10:03	2024-02-03 02:00	2023-06-30	2024-06-29
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.161	443	2022-08-29 09:37	2024-02-03 02:00	2023-06-30	2024-06-29
SUB_ORG	Backup Files Disclosure	Medium	x.x.85.123	443	2023-08-10 18:10	2024-02-04 01:33	2024-01-11	2024-06-30
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.88.138	443	2023-09-12 06:52	2024-02-03 00:22	2023-09-20	2024-06-30
SUB_ORG	TLS Version 1.0 Protocol Detection	High	x.x.85.123	443	2018-07-01 20:13	2023-11-11 23:58	2023-11-11	2024-07-01
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.123	443	2023-06-14 11:26	2024-02-04 01:33	2023-07-06	2024-07-05
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.186.112	443	2023-06-17 03:50	2024-02-03 01:50	2023-07-06	2024-07-05
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.160	443	2023-06-15 15:28	2024-02-04 05:04	2024-01-19	2024-07-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.158	443	2023-06-29 06:19	2024-02-02 21:40	2023-09-27	2024-07-23
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.157	443	2023-06-30 20:34	2024-02-02 17:56	2023-09-27	2024-07-23
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.232	443	2012-11-27 10:21	2024-02-03 00:08	2023-07-26	2024-07-25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.232	443	2017-06-08 02:25	2024-02-03 00:08	2023-07-26	2024-07-25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.89.152	443	2018-09-09 19:47	2024-02-03 01:48	2023-07-26	2024-07-25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.89.152	443	2018-09-09 19:47	2024-02-03 01:48	2023-07-26	2024-07-25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.233	443	2021-10-05 23:51	2024-02-03 22:30	2023-07-26	2024-07-25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.233	443	2021-10-05 23:51	2024-02-03 22:30	2023-07-26	2024-07-25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.89.153	443	2021-10-07 01:59	2024-02-04 04:20	2023-07-26	2024-07-25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.159	443	2023-03-16 23:07	2024-02-04 05:17	2023-09-27	2024-08-03
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.177	443	2023-07-25 01:01	2024-01-28 01:39	2023-08-04	2024-08-03
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.216	443	2023-07-27 12:43	2024-02-04 02:29	2023-08-04	2024-08-03
SUB_ORG	Drupal PHPUnit/Mailchimp Code Execution Vulnerability	Critical	x.x.58.55	443	2023-07-22 18:55	2023-10-04 15:11	2023-08-07	2024-08-06
SUB_ORG	Spring Framework Spring4Shell (CVE-2022-22965)	Critical	x.x.80.53	443	2022-04-12 01:16	2023-12-09 17:43	2023-08-11	2024-08-10
SUB_ORG	Spring Framework Spring4Shell (CVE-2022-22965)	Critical	x.x.165.41	443	2022-04-13 07:50	2023-12-09 11:54	2023-08-11	2024-08-10
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.11.141	8083	2023-08-02 15:56	2024-02-03 03:20	2023-08-15	2024-08-14
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.11.140	8443	2023-08-02 16:22	2024-02-03 00:22	2023-08-15	2024-08-14
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.11.140	8444	2023-08-02 16:22	2024-02-03 00:22	2023-08-15	2024-08-14
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.11.140	10002	2023-08-02 16:22	2024-02-03 00:22	2023-08-15	2024-08-14
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.11.140	8081	2023-08-02 16:22	2024-02-03 00:22	2023-08-15	2024-08-14
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.11.140	20000	2023-08-02 16:22	2024-02-03 00:22	2023-08-15	2024-08-14
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.30	443	2016-09-02 14:25	2024-02-03 01:52	2023-09-20	2024-08-15
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.10	443	2021-10-13 14:47	2024-02-04 01:17	2023-09-20	2024-09-01
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.172	443	2022-06-26 11:30	2024-02-04 03:44	2023-09-22	2024-09-21

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	False Positive Effective	False Positive Expiration
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.49.231	443	2023-05-19 17:33	2024-02-04 04:30	2023-10-16	2024-10-15
SUB_ORG	TLS Version 1.0 Protocol Detection	Medium	x.x.49.231	443	2023-07-10 15:50	2024-02-04 04:30	2023-10-16	2024-10-15
SUB_ORG	Backup Files Disclosure	Medium	x.x.57.150	443	2023-10-25 12:48	2024-02-03 01:20	2023-12-05	2024-11-03
SUB_ORG	OpenSSL 1.1.1 < 1.1.1o Vulnerability	Critical	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1p Vulnerability	Critical	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1o Vulnerability	Critical	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1p Vulnerability	Critical	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1l Vulnerability	High	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1n Vulnerability	High	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1t Multiple Vulnerabilities	High	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1l Vulnerability	High	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1n Vulnerability	High	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1t Multiple Vulnerabilities	High	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.58.17	443	2023-08-23 16:32	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.26	443	2023-08-23 22:53	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1m Vulnerability	Medium	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1q Vulnerability	Medium	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities	Medium	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1v Vulnerability	Medium	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1m Vulnerability	Medium	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1q Vulnerability	Medium	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities	Medium	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1v Vulnerability	Medium	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities	Medium	x.x.58.17	443	2023-10-19 22:09	2023-11-28 00:45	2023-11-14	2024-11-13
SUB_ORG	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities	Medium	x.x.50.26	443	2023-10-19 22:18	2023-11-28 00:52	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1x Vulnerability	Medium	x.x.50.26	443	2023-11-07 23:40	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1x Vulnerability	Medium	x.x.58.17	443	2023-11-08 00:35	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.125.62	443	2023-12-13 10:13	2024-01-31 22:31	2023-12-21	2024-12-03
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.60.32	443	2022-10-01 00:13	2024-02-04 00:44	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.234	443	2022-10-01 12:17	2024-02-02 21:56	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.234	49443	2022-10-01 12:17	2024-02-02 21:56	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.231	49443	2022-10-01 12:32	2024-02-02 21:12	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.231	443	2022-10-01 12:32	2024-02-02 21:12	2023-12-08	2024-12-07

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	False Positive Effective	False Positive Expiration
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.232	443	2022-10-09 09:36	2024-02-03 01:37	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.232	49443	2022-10-09 09:36	2024-02-03 01:37	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.233	49443	2022-10-09 09:54	2024-02-03 02:07	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.233	443	2022-10-09 09:54	2024-02-03 02:07	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.60.31	443	2022-10-09 11:29	2024-02-03 02:27	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.59.87	443	2023-03-30 11:25	2024-02-04 00:27	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.182	443	2023-03-30 17:35	2024-02-04 00:30	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.182	49443	2023-05-11 23:00	2024-02-04 00:30	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.166	443	2023-06-22 09:50	2024-02-02 19:14	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.59.87	49443	2023-08-11 15:15	2024-02-04 00:27	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.167	443	2023-08-23 09:17	2024-02-04 07:11	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.60.32	49443	2023-09-07 13:19	2024-02-04 00:44	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.60.31	49443	2023-09-08 22:32	2024-02-03 02:27	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.95.28	443	2023-06-19 21:51	2024-02-04 04:44	2024-01-25	2025-01-24
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.164	443	2023-09-23 00:29	2024-02-04 03:02	2024-01-25	2025-01-24
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.87.28	443	2023-09-27 16:43	2024-02-04 05:24	2024-01-25	2025-01-24

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, please complete and return the False Positive Assertion Form found in Appendix G: Attachments to CISA.
   - CISA 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 the report for one year. Vulnerabilities marked as 'false positive' will be reported in Appendix E: False Positive Findings, along with the dates of when the false positive took effect and when it will expire.
   - CISA reserves the right to assert that certain findings are not false positives, and when false positive assertions are accepted by CISA, 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 CISA 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 CISA.
     - 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. CISA 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 vulnerability@cisa.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. CISA 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 Report Card?	Listed in Appendix 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, however, we are looking into adding this feature in the future.

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. CISA 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 vulnerability@cisa.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 vulnerability@cisa.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 8.2: Methodology / Process.

15. **I own a 2nd-level domain that is not represented in my certificate data.**

    - If you believe we are missing 2nd-level domains, you can reach out to vulnerability@cisa.dhs.gov and request that we add them to our domain gatherer.

Appendix G Attachments

If your PDF viewer supports embedded attachments you will see paper clip icons below for each attached file which includes additional report details. To access the attachments embedded within the report, open the report with a dedicated PDF reader (such as Adobe Acrobat), and click on the paper clip icon to the left of the attachment name.

- certificates.csv : Data collected about each certificate found that was issued for a domain known to belong to you.
- cyber-hygiene-data-sharing-form.pdf: Form to request your weekly findings be shared with a trusted third party (e.g. MSP, ISAC, Consultant, etc.); send the completed form to vulnerability@cisa.dhs.gov.
- cyber-hygiene-false-positive-assertion-form.pdf: Form to request that one or more vulnerabilities be marked as false positives; send the completed form to vulnerability@cisa.dhs.gov.
- days-currently-active.csv: Metrics over time for median and maximum age of active vulnerabilities (active as of date listed in each row).
- 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).
- domains.csv : A CSV containing all the base domains we know belong to you.
- false-positive-findings.csv : List of all reported false positive vulnerability findings.
- findings.csv : Detailed list of all vulnerability findings for each IP address and port.
- hosts.csv : List of hosts discovered with IP address, best-guess OS identification, and hostname if available.
- mitigated-vulnerabilities.csv : List of vulnerabilities that were included on the last report, but were not detected in the latest scans.
- potentially-risky-services.csv : List of all potentially risky services detected and the associated IP address and port.
- recently-detected.csv : List of all vulnerabilities detected since the last report, but not detected in the latest scans.
- scope.csv : List of IP addresses that were in scope for this report.
- services.csv : List of all discovered services and the associated IP address and port. NOTE: This attachment excludes the 1,986,714 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.
- sub-org-summary.csv : Data from the Sub-Organization Summary.

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. 11, 18

false positive Any normal or expected behavior that is identified in this report as a potentially exploitable vulnerability. 10, 18, 42, 47, 50

host A device that has a least one open port/listening service. 5, 10, 14, 15, 17–19, 22, 41, 47, 50

host scan A scan of all assets to identify hosts. 6

initial detection The initial point in time when Cyber Hygiene scans identified a vulnerability. This date is used to calculate the vulnerability's age. 11, 12, 15, 25–27

known exploited vulnerability A vulnerability listed in CISA's catalog of known exploited vulnerabilities. For more information, please refer to Section 3: Binding Operational Directive 22-01 — Reducing the Significant Risk of Known Exploited Vulnerabilities. 7

latest detection The most recent time when Cyber Hygiene scans identified a particular vulnerability. 26, 27

mitigation detection The date when a previously identified vulnerability was no longer detected by Cyber Hygiene scans. 25

service An application running at the network application layer that provides communications capabilities across an IP computer network. 5, 14, 15, 21, 50

severity Please review the following guide for vulnerability severity scoring information: https://www.first.org/cvss/v2/guide. 5, 15, 19, 22, 24

vulnerability A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. 5, 7, 10–12, 14, 15, 18, 19, 21–28, 41, 42, 47, 50

vulnerability age The time between a vulnerability's initial detection date and its latest detection date. 11, 12, 15, 49

vulnerability scan A vulnerability scan on all hosts identified during host scan. 6

vulnerable host A host with at least one vulnerability detected on the most recent scan used for this report. 22

Acronyms

AWS Amazon Web Services. 14

CIRCIA Cyber Incident Reporting for Critical Infrastructure Act of 2022. 7

CISA Cybersecurity and Infrastructure Security Agency [https://www.cisa.gov]. 5, 7–10, 14, 15, 18, 23, 42, 47, 48

CSV Comma-Separated Values. 5, 13, 14, 47, 50

CT Certificate transparency. 9

CVE Common Vulnerabilities and Exposures; for more information refer to https://cve.mitre.org/about/faqs.html. 7, 16

CVSS Common Vulnerability Scoring System; for more information refer to https://www.first.org/cvss/v2. 4, 16, 18, 19

CyHy Cyber Hygiene. 5, 10–14, 16, 18, 20, 47, 48

DNS Domain Name Service. 9

HTTPS Hypertext Transfer Protocol Secure. 48

IP Internet Protocol. 14, 48, 50

IT Information Technology. 10

KEV Known Exploited Vulnerability. 7

NVD National Vulnerability Database; for more information refer to https://nvd.nist.gov. 16

OS Operating System. 14, 50

POA&M Plan Of Action and Milestones. 47

RRS Risk Rating System. 19

RVWP Ransomware Vulnerability Warning Pilot. 7

SAMPLE Sample Organization. 5, 10–14, 17, 18, 21–23, 42

TCP Transmission Control Protocol. 14, 50