SAMPLE-STR-2025

Confidential Property of Sample Financial Institution

2025-XX-XX

RESCOR LLC
521 Lincoln Road
West Enfield, ME 04493 USA

Generated on: 2025-XX-XX

Table of Contents

Executive Summary

↑ Table of Contents

Between 2025-XX-XX and 2025-XX-XX, RESCOR LLC (“RESCOR”) conducted security testing (“the test”) on selected information processing resources of Sample Financial Institution (“the Institution”). Based on findings from the test, the Institution has much lower exposure to technical vulnerabilities when compared with organizations that have undergone similar testing. Chart 1 depicts the breakdown of findings by severity.

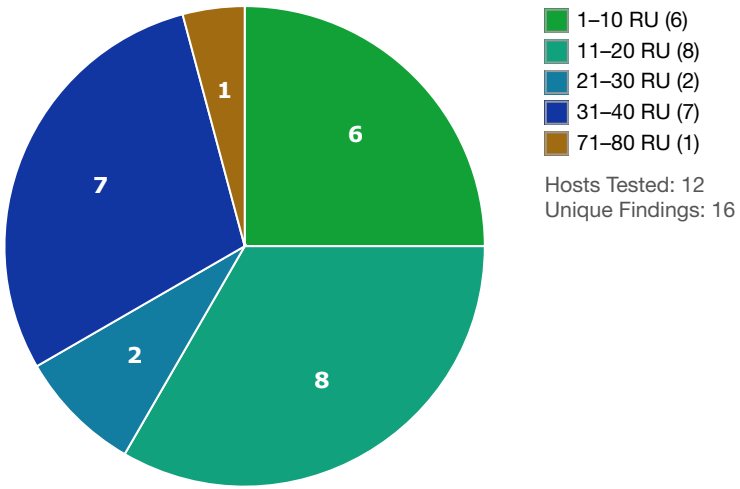
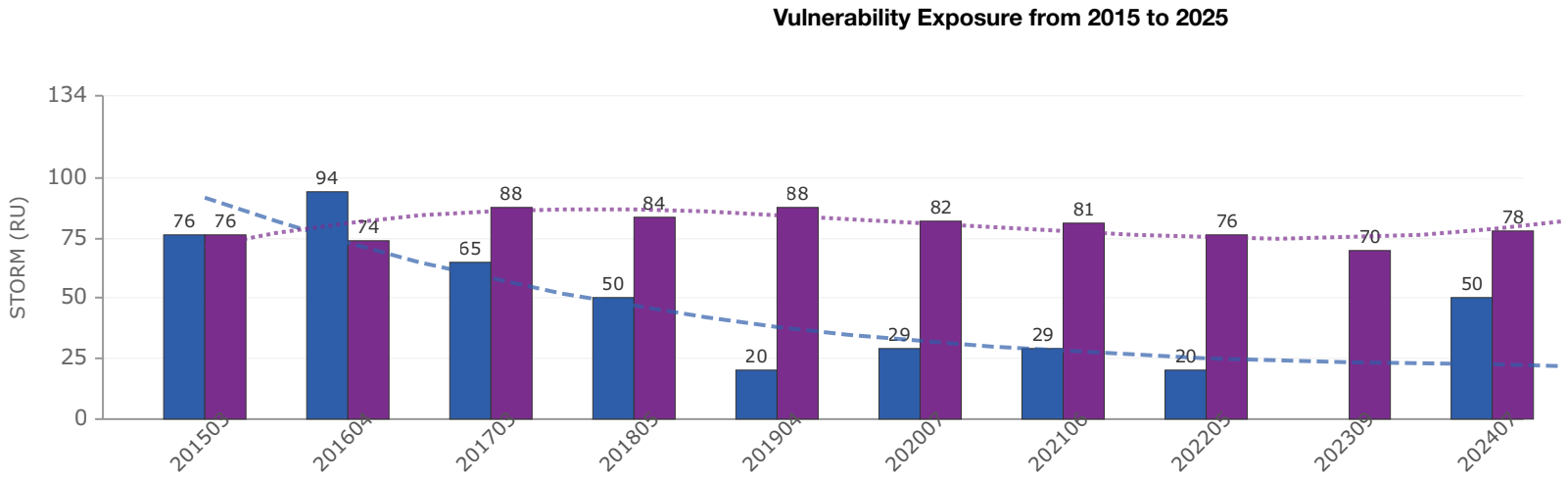


Chart 1 — Findings by Severity

Chart 2 depicts the vulnerability exposure trend over time.



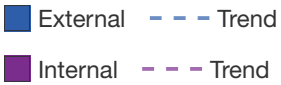


Chart 2 — Vulnerability Exposure Over Time

1. *the Institution's external (Internet) presence has an exposure in the 1st percentile of similar organizations.* Of 48 similar tests the average exposure is 67 RU compared to the Institution's 5 RU (99% of similar organizations have equal or greater exposure), and the trend of exposure is ***stable***.
2. *the Institution's internal network has an exposure in the 25th percentile of similar organizations.* Of 57 similar tests the average exposure is 107 RU compared to the Institution's 89 RU (75% of similar organizations have equal or greater exposure), and the trend of exposure is ***increasing***.

Top Vulnerabilities

Source	ID	Finding	Severity
OpenVAS	103674	Operating System (OS) End of Life (EOL) Detection	75 RU
OpenVAS	117687	Weak Host Key Algorithm(s) (SSH)	40 RU
OpenVAS	150713	Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	40 RU
OpenVAS	80089	Sybase ASA Ping	38 RU
OpenVAS	103955	SSL/TLS: Certificate Expired	38 RU
OpenVAS	117761	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	38 RU
OpenVAS	117274	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	33 RU
OpenVAS	106223	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabilit…	30 RU
OpenVAS	80091	TCP Timestamps Information Disclosure	20 RU
OpenVAS	105610	Weak MAC Algorithm(s) Supported (SSH)	20 RU

6 additional findings detailed in the Vulnerability Detail section (findings below 5 RU are omitted from that section).

Summary of Recommendations

Where shown, the highlighted values indicate the projected horizon severity reduction (before → after) in Risk Units if the recommendation is implemented.

External Recommendations

1. No Remediation Required for Internet Host Visibility Findings `5 → 0 RU`

Internal Recommendations

1. Replace End-of-Life Unifi Cloud Key II Running Obsolete Ubuntu `89 → 53 RU`
2. Disable Weak SSL/TLS Protocols and Harden SSH Cryptographic Configuration `53 → 45 RU`
3. Disable Sybase ASA Ping Responses on the Domain Controller `45 → 26 RU`
4. Defer Low-Priority Internal Network Findings Until Higher Risks Are Resolved `26 → 0 RU`

External Recommendations

↑ Table of Contents

1. **No Remediation Required for Internet Host Visibility Findings**

   The findings under OS Detection Consolidation and Reporting and Hostname Determination Reporting are informational observations reflecting normal internet-facing host visibility. No vulnerabilities were detected on these hosts, and no configuration changes are required.

   If this recommendation is followed, the vulnerability severity for this horizon will be reduced from 5 RU to 0 RU (5 RU impact).

Source	ID	Finding	Severity (RU)
OpenVAS	105937	OS Detection Consolidation and Reporting	4 RU
OpenVAS	108449	Hostname Determination Reporting	4 RU

Internal Recommendations

↑ Table of Contents

1. **Replace End-of-Life Unifi Cloud Key II Running Obsolete Ubuntu**

   The Unifi Cloud Key II is running an end-of-life version of Ubuntu Linux, as identified under Operating System (OS) End of Life (EOL) Detection. EOL operating systems no longer receive security patches, leaving the device permanently exposed to known vulnerabilities. Complete the in-progress device replacement with the vendor to fully remediate this finding.

   If this recommendation is followed, the vulnerability severity for this horizon will be reduced from 89 RU to 53 RU (36 RU impact).

Source	ID	Finding	Severity (RU)
OpenVAS	103674	Operating System (OS) End of Life (EOL) Detection	75 RU

2. **Disable Weak SSL/TLS Protocols and Harden SSH Cryptographic Configuration**

   Multiple findings — including Deprecated TLSv1.0 and TLSv1.1 Protocol Detection, SSL/TLS Certificate Expired, Diffie-Hellman Insufficient DH Group Strength, SSL/TLS Renegotiation DoS Vulnerability, and weak SSH host key algorithms, KEX algorithms, and MAC algorithms — collectively indicate that outdated and insecure cryptographic configurations are in use across overlapping systems. Disable TLSv1.0 and TLSv1.1 on all affected hosts, renew all expired or self-signed certificates, and enforce strong DH groups and TLS renegotiation controls. On all affected SSH daemons, update to a current version and restrict configurations to approved ciphers, MAC algorithms, and key exchange algorithms. Address both SSL/TLS and SSH hardening together in a single change window, as they affect the same systems and are owned by the same infrastructure team.

   If this recommendation is followed, the vulnerability severity for this horizon will be reduced from 53 RU to 45 RU (8 RU impact).

Source	ID	Finding	Severity (RU)
OpenVAS	117687	Weak Host Key Algorithm(s) (SSH)	40 RU
OpenVAS	150713	Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	40 RU
OpenVAS	103955	SSL/TLS: Certificate Expired	38 RU
OpenVAS	117761	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	38 RU
OpenVAS	117274	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	33 RU
OpenVAS	106223	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	30 RU

OpenVAS	105610	Weak MAC Algorithm(s) Supported (SSH)	20 RU

3. **Disable Sybase ASA Ping Responses on the Domain Controller**

   The domain controller appears to be running Sybase Adaptive Server Anywhere (ASA), which is responding to ASA ping requests and disclosing system information, as identified under Sybase ASA Ping. If no Institution applications depend on ASA ping functionality, disable ping responses by adding the -sb 0 option to the Sybase server startup configuration. If ASA ping is actively used by an application, document and formally accept this risk.

   If this recommendation is followed, the vulnerability severity for this horizon will be reduced from 45 RU to 26 RU (19 RU impact).

Source	ID	Finding	Severity (RU)
OpenVAS	80089	Sybase ASA Ping	38 RU

4. **Defer Low-Priority Internal Network Findings Until Higher Risks Are Resolved**

   The findings covering TCP Timestamps Information Disclosure, DCE/RPC and MSRPC Services Enumeration Reporting, Missing HttpOnly Cookie Attribute, DNS Cache Snooping, and ICMP Timestamp Reply Information Disclosure represent theoretical information-disclosure risks on an internal network. On internal infrastructure, the configuration changes required to address these findings may introduce instability that outweighs the benefit at this time. Revisit these items after all higher-severity findings have been remediated.

   If this recommendation is followed, the vulnerability severity for this horizon will be reduced from 26 RU to 0 RU (26 RU impact).

Source	ID	Finding	Severity (RU)
OpenVAS	80091	TCP Timestamps Information Disclosure	20 RU
OpenVAS	10736	DCE/RPC and MSRPC Services Enumeration Reporting	19 RU
OpenVAS	105925	Missing 'HttpOnly' Cookie Attribute (HTTP)	19 RU
OpenVAS	146591	DNS Cache Snooping Vulnerability (UDP) - Active Check	19 RU
OpenVAS	103190	ICMP Timestamp Reply Information Disclosure	16 RU

Host Table

↑ Table of Contents

This section lists hosts by horizon (external and internal) and descending vulnerability severity. If you are viewing this report in web format (HTML), you can click on the IP address of a host to view its host detail.

Horizon	Address	Name	Profile?	Host RU
External	198.51.100.10	198-51-100-10.host01.region1.example.net	198.51.100.10	5 RU
External	198.51.100.11	198-51-100-11.host01.region1.example.net	198.51.100.10	5 RU
Internal	10.0.2.1	controller.sample.local		89 RU
Internal	10.0.1.100			48 RU
Internal	10.0.1.10	sample-file01.sample.local		46 RU
Internal	10.0.2.20	unifi		38 RU
Internal	10.0.1.11	sample-dc01.sample.local		24 RU
Internal	10.0.1.20	sample-iot01.sample.local		20 RU
Internal	10.0.2.24	sample-lptp-01.sampleext.local	10.0.1.30	20 RU
Internal	10.0.2.172		10.0.1.21	16 RU
Internal	10.0.1.30		10.0.1.30	10 RU
Internal	10.0.1.21		10.0.1.21	8 RU

External Host Details

↑ Table of Contents

The following section contains detailed information on the 2 hosts on the External horizon. (1 additional hosts are represented by profiles below)

198.51.100.10 198-51-100-10.host01.region1.example.net 5 RU

Profile 198.51.100.10 (198-51-100-10.host01.region1.example.net) has a vulnerability severity of 5 RU (low severity) based on 2 findings. There are no remedial annotations that affect this result (the vulnerability severity measurements include reductions for any remedial actions documented below).

Profile Summary

This host is a representative member of a "profile" that contains 2 hosts that all have the same list of vulnerabilities. The addresses of these hosts appear in the table below.

198.51.100.10 198.51.100.11

Vulnerabilities

Source	ID	Title	Original RU	Corrected RU
OpenVAS	105937	OS Detection Consolidation and Reporting No Best matching OS identified. Please see the VT 'Unknown OS and Service Banner Reporting' (OID: 1.3.6.1.4.1.25623.1.0.108441) for possible ways to identify this OS.	5 RU	4 RU
OpenVAS	108449	Hostname Determination Reporting Hostname determination for IP 198.51.100.10: Hostname|Source 198-51-100-10.host01.region1.example.net|Reverse-DNS	5 RU	4 RU

Identities

ID	Name Type	Name
0	DNS PTR	198-51-100-10.host01.region1.example.net

Internal Host Details

↑ Table of Contents

The following section contains detailed information on the 10 hosts on the Internal horizon. (2 additional hosts are represented by profiles below)

10.0.2.1	controller.sample.local	89 RU

Host 10.0.2.1 (controller.sample.local) has a vulnerability severity of 89 RU (high severity) based on 8 findings. There are 2 remedial annotations that affect this result (the vulnerability severity measurements include reductions for any remedial actions documented below).

Vulnerabilities

Source	ID	Title	Original RU	Corrected RU
OpenVAS	103674	Operating System (OS) End of Life (EOL) Detection The "Debian GNU/Linux" Operating System on the remote host has reached the end of life. CPE: cpe:/o:debian:debian_linux:7 Installed version, build or SP: 7 EOL date: 2018-05-31 EOL info: …	100 RU	75 RU

Source	ID	Title	Original RU	Corrected RU
OpenVAS	117687	Weak Host Key Algorithm(s) (SSH) The remote SSH server supports the following weak host key algorithm(s): host key algorithm | Description ---------- ssh-dss | Digital Signature Algorithm (DSA) /…	53 RU	40 RU
OpenVAS	150713	Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) The remote SSH server supports the following weak KEX algorithm(s): KEX algorithm | Reason ---------- diffie-hellman-group-exchange-sha1 | Using…	53 RU	40 RU
OpenVAS	117274	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067)…	43 RU	33 RU
OpenVAS	106223	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability Server Temporary Key Size: 1024 bits	40 RU	30 RU
OpenVAS	105610	Weak MAC Algorithm(s) Supported (SSH) The remote SSH server supports the following weak client-to-server MAC algorithm(s): umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC…	26 RU	20 RU
OpenVAS	105925	Missing 'HttpOnly' Cookie Attribute (HTTP) The cookie(s): Set-Cookie: PHPSESSID=***replaced***; path=/; secure is/are missing the "HttpOnly" cookie attribute.	50 RU	19 RU

Source	ID	Title	Original RU	Corrected RU

OpenVAS	146591	DNS Cache Snooping Vulnerability (UDP) - Active Check
		`Received (an) answer(s) for a non-recursive query for "example.com".`
		`Result:`
		`198.51.100.20`
			50 RU	19 RU

Remedial Annotations

Source	ID	Description	Remedial %
OpenVAS	146591	Curing these vulnerabilities may cause more harm than good - save these for later	50%
OpenVAS	105925	Curing these vulnerabilities may cause more harm than good - save these for later	50%

Identities

ID	Name Type	Name
0	DNS PTR	controller.sample.local

10.0.1.100 — 48 RU

Host 10.0.1.100 has a vulnerability severity of 48 RU (medium severity) based on 2 findings. There are no remedial annotations that affect this result (the vulnerability severity measurements include reductions for any remedial actions documented below).

Vulnerabilities

Source	ID	Title	Original RU	Corrected RU

OpenVAS	103955	SSL/TLS: Certificate Expired
		`The certificate of the remote service expired on 2025-XX-XX 00:00:00.`
		`Certificate details:`
		`fingerprint (SHA-1) | A1B2C3D4E5F6A1B2C3D4E5F6A1B2C3D4E5F6A1B2`
		`fingerprint (SHA-256) |…`
			50 RU	38 RU

OpenVAS	117761	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
		`The following indicates that the remote SSL/TLS service is affected:`
		`Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an existing / already established SSL/TLS…`
			50 RU	38 RU

10.0.1.10 sample-file01.sample.local 46 RU

Host 10.0.1.10 (sample-file01.sample.local) has a vulnerability severity of 46 RU (medium severity) based on 2 findings. There are no remedial annotations that affect this result (the vulnerability severity measurements include reductions for any remedial actions documented below).

Vulnerabilities

Source	ID	Title	Original RU	Corrected RU

OpenVAS	80089	Sybase ASA Ping
		`Database name: sample-file01_payclock`
		`Database port: 2638`
			50 RU	38 RU

OpenVAS	106223	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability `Server Temporary Key Size: 1024 bits`	40 RU	30 RU

Identities

ID	Name Type	Name
0	DNS PTR	sample-file01.sample.local

10.0.2.20 unifi 38 RU

Host 10.0.2.20 (unifi) has a vulnerability severity of 38 RU (low severity) based on 1 finding. There are no remedial annotations that affect this result (the vulnerability severity measurements include reductions for any remedial actions documented below).

Vulnerabilities

Source	ID	Title	Original RU	Corrected RU

OpenVAS	103955	SSL/TLS: Certificate Expired
		`The certificate of the remote service expired on 2021-03-17 20:33:40.`
		
		`Certificate details:`
		`fingerprint (SHA-1) | F6E5D4C3B2A1F6E5D4C3B2A1F6E5D4C3B2A1F6E5`
		`fingerprint (SHA-256) |…`
			50 RU	38 RU

Identities

ID	Name Type	Name
0	DNS PTR	unifi

10.0.1.11	sample-dc01.sample.local, sample-server.sample.local	24 RU

Host 10.0.1.11 (sample-dc01.sample.local) has a vulnerability severity of 24 RU (low severity) based on 2 findings. There are 2 remedial annotations that affect this result (the vulnerability severity measurements include reductions for any remedial actions documented below).

Vulnerabilities

Source	ID	Title	Original RU	Corrected RU

OpenVAS	10736	DCE/RPC and MSRPC Services Enumeration Reporting
		`Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:`
		`Port: 1536/tcp`
		`UUID: a1b2c3d4-e5f6-7890-abcd-ef1234567890, version 1`
		`Endpoint: ncacn_ip_tcp:10.0.1.11[1536]`
		`Port: 1537/tcp`
		`UUID:…`
			50 RU	19 RU

OpenVAS	146591	DNS Cache Snooping Vulnerability (UDP) - Active Check
		`Received (an) answer(s) for a non-recursive query for "example.com".`
		`Result:`
		`198.51.100.30`
			50 RU	19 RU

Remedial Annotations

Source	ID	Description	Remedial %
OpenVAS	146591	Curing these vulnerabilities may cause more harm than good - save these for later	50%
OpenVAS	10736	Curing these vulnerabilities may cause more harm than good - save these for later	50%

Identities

ID	Name Type	Name
0	DNS PTR	sample-dc01.sample.local
	DNS PTR	sample-server.sample.local

10.0.1.20 sample-iot01.sample.local 20 RU

Host 10.0.1.20 (sample-iot01.sample.local) has a vulnerability severity of 20 RU (low severity) based on 1 finding. There are no remedial annotations that affect this result (the vulnerability severity measurements include reductions for any remedial actions documented below).

Vulnerabilities

Source	ID	Title	Original RU	Corrected RU

OpenVAS	105610	Weak MAC Algorithm(s) Supported (SSH)
		`The remote SSH server supports the following weak client-to-server MAC algorithm(s):`
		
		`umac-64-etm@openssh.com`
		`umac-64@openssh.com`
		
		`The remote SSH server supports the following weak server-to-client MAC…`
			26 RU	20 RU

Identities

ID	Name Type	Name
0	DNS PTR	sample-iot01.sample.local

10.0.1.30 10 RU

Profile 10.0.1.30 has a vulnerability severity of 10 RU (low severity) based on 1 finding. There are 2 remedial annotations that affect this result (the vulnerability severity measurements include reductions for any remedial actions documented below).

Profile Summary

This host is a representative member of a "profile" that contains 2 hosts that all have the same list of vulnerabilities. The addresses of these hosts appear in the table below.

10.0.1.30 10.0.2.24

Vulnerabilities

Source	ID	Title	Original RU	Corrected RU

OpenVAS	80091	TCP Timestamps Information Disclosure
		`It was detected that the host implements RFC1323/RFC7323.`
		
		`The following timestamps were retrieved with a delay of 1 seconds in-between:`
		`Packet 1: 186170910`
		`Packet 2: 186171965`
			26 RU	10 RU

Remedial Annotations

Source	ID	Description	Remedial %
OpenVAS	80091	Curing these vulnerabilities may cause more harm than good - save these for later	50%
OpenVAS	80091	This profile MAY represent the same host connected to both the LAN and WiFi	0%

10.0.1.21 — 8 RU

Profile 10.0.1.21 has a vulnerability severity of 8 RU (low severity) based on 1 finding. There are 2 remedial annotations that affect this result (the vulnerability severity measurements include reductions for any remedial actions documented below).

Profile Summary

This host is a representative member of a "profile" that contains 2 hosts that all have the same list of vulnerabilities. The addresses of these hosts appear in the table below.

10.0.1.21 10.0.2.172

Vulnerabilities

Source	ID	Title	Original RU	Corrected RU

OpenVAS	103190	ICMP Timestamp Reply Information Disclosure
		`The following response / ICMP packet has been received:`
		`- ICMP Type: 14`
		`- ICMP Code: 0`
			21 RU	8 RU

Remedial Annotations

Source	ID	Description	Remedial %
OpenVAS	103190	Curing these vulnerabilities may cause more harm than good - save these for later	50%
OpenVAS	103190	This profile MAY represent the same host connected to both the LAN and WiFi	0%

Vulnerability Detail

↑ Table of Contents

This section describes each unique vulnerability discovered during the test, along with the hosts affected.

2 findings with a severity below 5 RU have been omitted from this section.

OpenVAS 103674	Operating System (OS) End of Life (EOL) Detection	75 RU

Title

Operating System (OS) End of Life (EOL) Detection

Description

The Operating System (OS) on the remote host has reached the end
of life (EOL) and should not be used anymore.

Solution

Update the OS on the remote host to a version which is still
supported and receiving security updates by the vendor.

Note / Important: Please create an override for this result if the target host is a:

- Windows system with Extended Security Updates (ESU)

- System with additional 3rd-party / non-vendor security updates like e.g. from 'TuxCare',
'Freexian Extended LTS' or similar

Impact on Target

An EOL version of an OS is not receiving any security updates
from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise
the security of this host.

Method of Detection

Checks if an EOL version of an OS is present on the target
host.

Affected Hosts

10.0.2.1

OpenVAS 117687	Weak Host Key Algorithm(s) (SSH)	40 RU

Title

Weak Host Key Algorithm(s) (SSH)

Description

The remote SSH server is configured to allow / support weak host key algorithm(s).

Solution

Disable the reported weak host key algorithm(s).

Method of Detection

Checks the supported host key algorithms of the remote SSH server.

Currently weak host key algorithms are defined as the following:

- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)

Affected Hosts

10.0.2.1

OpenVAS 150713	Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	40 RU

Title

Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Description

The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Tech Description

- 1024-bit MODP group / prime KEX algorithms:

Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.

A nation-state can break a 1024-bit prime.

Solution

Disable the reported weak KEX algorithm(s)

- 1024-bit MODP group / prime KEX algorithms:

Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Impact on Target

An attacker can quickly break individual connections.

Method of Detection

Checks the supported KEX algorithms of the remote SSH server.

Currently weak KEX algorithms are defined as the following:

- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime

- ephemerally generated key exchange groups uses SHA-1

- using RSA 1024-bit modulus key

Affected Hosts

10.0.2.1

OpenVAS 80089 — Sybase ASA Ping — 38 RU

Title

Sybase ASA Ping

Description

The remote Sybase SQL Anywhere / Adaptive Server Anywhere database is
configured to listen for client connection broadcasts, which allows an attacker to see the name and port
that the Sybase SQL Anywhere / Adaptive Server Anywhere server is running on.

Solution

Switch off broadcast listening via the '-sb' switch when starting
Sybase.

Affected Hosts

10.0.1.10

OpenVAS 103955 — SSL/TLS: Certificate Expired — 38 RU

Title

SSL/TLS: Certificate Expired

Description

The remote server's SSL/TLS certificate has already expired.

Tech Description

This script checks expiry dates of certificates associated with
SSL/TLS-enabled services on the target and reports whether any have already expired.

Solution

Replace the SSL/TLS certificate by a new one.

Affected Hosts

10.0.1.100 10.0.2.20

OpenVAS 117761	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473,…	38 RU

Title

SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

Description

The remote SSL/TLS service is prone to a denial of service (DoS)
vulnerability.

Tech Description

The flaw exists because the remote SSL/TLS service does not
properly restrict client-initiated renegotiation within the SSL and TLS protocols.

Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but
both are in a DISPUTED state with the following rationale:

> It can also be argued that it is the responsibility of server deployments, not a security
library, to prevent or limit renegotiation when it is inappropriate within a specific environment.

Both CVEs are still kept in this VT as a reference to the origin of this flaw.

Solution

Users should contact their vendors for specific patch information.

A general solution is to remove/disable renegotiation capabilities altogether from/in the affected
SSL/TLS service.

Impact on Target

The flaw might make it easier for remote attackers to cause a
DoS (CPU consumption) by performing many renegotiations within a single connection.

Method of Detection

Checks if the remote service allows to re-do the same SSL/TLS
handshake (Renegotiation) over an existing / already established SSL/TLS connection.

Affected Applications & Platforms

Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

Affected Hosts

10.0.1.100

OpenVAS 117274	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	33 RU

Title

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Description

It was possible to detect the usage of the deprecated TLSv1.0
and/or TLSv1.1 protocol on this system.

Tech Description

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic
flaws like:

- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)

- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy
Encryption (FREAK)

Solution

It is recommended to disable the deprecated TLSv1.0 and/or
TLSv1.1 protocols in favor of the TLSv1.2+ protocols.

Please see the references for more resources supporting you with this task.

Impact on Target

An attacker might be able to use the known cryptographic flaws to
eavesdrop the connection between clients and the service to get access to sensitive data
transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates
anymore.

Method of Detection

Checks the used TLS protocols of the services provided by this
system.

Affected Applications & Platforms

- All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols

- CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder

- CVE-2024-41270: Gorush v1.18.4

- CVE-2025-3200: Multiple products from Wiesemann & Theis

References

CVE #	Title	CVSSA RSK
CVE-2011-3389		0 RU
CVE-2015-0204		0 RU
CVE-2023-41928		0 RU
CVE-2024-41270		0 RU
CVE-2025-3200		0 RU

Affected Hosts

10.0.2.1

OpenVAS 106223	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group…	30 RU

Title

SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Description

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength
(key size < 2048).

Tech Description

The Diffie-Hellman group are some big numbers that are used as base for
the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size
of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really
powerful attackers like governments.

Solution

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use
a 2048-bit or stronger Diffie-Hellman group (see the references).

For Apache Web Servers:
Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Impact on Target

An attacker might be able to decrypt the SSL/TLS communication offline.

Method of Detection

Checks the DHE temporary public key size.

Affected Hosts

10.0.1.10 10.0.2.1

OpenVAS 80091	TCP Timestamps Information Disclosure	20 RU

Title

TCP Timestamps Information Disclosure

Description

The remote host implements TCP timestamps and therefore allows
to compute the uptime.

Tech Description

The remote host implements TCP timestamps, as defined by
RFC1323/RFC7323.

Solution

To disable TCP timestamps on linux add the line
'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at
runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when
initiating TCP connections, but use them if the TCP peer that is initiating communication includes
them in their synchronize (SYN) segment.

See the references for more information.

Impact on Target

A side effect of this feature is that the uptime of the remote
host can sometimes be computed.

Method of Detection

Special IP packets are forged and sent with a little delay in
between to the target IP. The responses are searched for a timestamps. If found, the timestamps
are reported.

Affected Applications & Platforms

TCP implementations that implement RFC1323/RFC7323.

Affected Hosts

10.0.1.30 10.0.2.24

OpenVAS 105610 | Weak MAC Algorithm(s) Supported (SSH) | 20 RU

Title

Weak MAC Algorithm(s) Supported (SSH)

Description

The remote SSH server is configured to allow / support weak MAC algorithm(s).

Solution

Disable the reported weak MAC algorithm(s).

Method of Detection

Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.

Currently weak MAC algorithms are defined as the following:

- MD5 based algorithms

- 96-bit based algorithms

- 64-bit based algorithms

- 'none' algorithm

Affected Hosts

10.0.1.20 10.0.2.1

OpenVAS 10736	DCE/RPC and MSRPC Services Enumeration Reporting	19 RU

Title

DCE/RPC and MSRPC Services Enumeration Reporting

Description

Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running
on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Solution

Filter incoming traffic to this ports.

Impact on Target

An attacker may use this fact to gain more knowledge
about the remote host.

Affected Hosts

10.0.1.11

OpenVAS 105925	Missing 'HttpOnly' Cookie Attribute (HTTP)	19 RU

Title

Missing 'HttpOnly' Cookie Attribute (HTTP)

Description

The remote HTTP web server / application is missing to set the
'HttpOnly' cookie attribute for one or more sent HTTP cookie.

Tech Description

The flaw exists if a session cookie is not using the 'HttpOnly'
cookie attribute.

This allows a cookie to be accessed by JavaScript which could lead to session hijacking
attacks.

Solution

- Set the 'HttpOnly' cookie attribute for any session cookie

- Evaluate / do an own assessment of the security impact on the web server / application and create
an override for this result if there is none (this can't be checked automatically by this VT)

Method of Detection

Checks all cookies sent by the remote HTTP web server /
application for a missing 'HttpOnly' cookie attribute.

Affected Applications & Platforms

Any web application with session handling in cookies.

Affected Hosts

10.0.2.1

OpenVAS 146591	DNS Cache Snooping Vulnerability (UDP) - Active Check	19 RU

Title

DNS Cache Snooping Vulnerability (UDP) - Active Check

Description

The DNS server is prone to a cache snooping vulnerability.

Tech Description

DNS cache snooping is when someone queries a DNS server in
order to find out (snoop) if the DNS server has a specific DNS record cached, and thereby
deduce if the DNS server's owner (or its users) have recently visited a specific site.

This may reveal information about the DNS server's owner, such as what vendor, bank, service
provider, etc. they use. Especially if this is confirmed (snooped) multiple times over a period.

This method could even be used to gather statistical information - for example at what time does
the DNS server's owner typically access his net bank etc. The cached DNS record's remaining TTL
value can provide very accurate data for this.

DNS cache snooping is possible even if the DNS server is not configured to resolve recursively
for 3rd parties, as long as it provides records from the cache also to 3rd parties (a.k.a.
'lame requests').

Solution

There are multiple possible mitigation steps depending on
location and functionality needed by the DNS server:

- Disable recursion

- Don't allow public access to DNS Servers doing recursion

- Leave recursion enabled if the DNS Server stays on a corporate network that cannot be reached
by untrusted clients

Impact on Target

Attackers might gain information about cached DNS records
which might lead to further attacks.

Note: This finding might be an acceptable risk if you:

- trust all clients which can reach the server

- do not allow recursive queries from outside your trusted client network.

Method of Detection

Sends a crafted DNS query and checks the response.

Affected Hosts

10.0.1.11 10.0.2.1

OpenVAS 103190	ICMP Timestamp Reply Information Disclosure	16 RU

Title

ICMP Timestamp Reply Information Disclosure

Description

The remote host responded to an ICMP timestamp request.

Tech Description

The Timestamp Reply is an ICMP message which replies to a
Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as
well as a receive timestamp and a transmit timestamp.

Solution

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely

- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in
either direction (either completely or only for untrusted networks)

Impact on Target

This information could theoretically be used to exploit weak
time-based random number generators in other services.

Method of Detection

Sends an ICMP Timestamp (Type 13) request and checks if a
Timestamp Reply (Type 14) is received.

Affected Hosts

10.0.1.21 10.0.2.172