YourIT!
Your Logo Goes Here

Technical Review

Internal Vulnerability Scan Results

Prepared for: Client Company

Prepared by: YourIT Company

YourIT!
Your Logo Goes Here

Table of Contents

Table of Contents

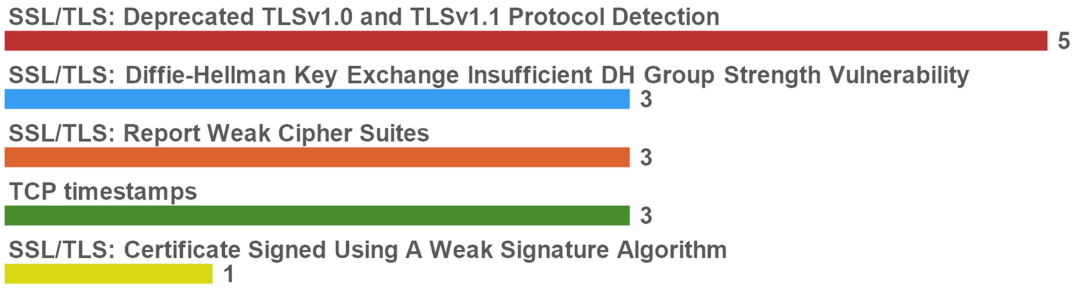
1 - Summary

This report gives details on hosts that were tested and issues that were found during the Internal Vulnerability Scan. The findings are grouped by category.

Appliances Used:
1. IVS-SEDY38

Issues by Severity

Issues by NVT



ISSUE	COUNT
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	5
TCP timestamps	3
SSL/TLS: Report Weak Cipher Suites	3
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	3
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	1

2 - Scan Details

This section details the issues discovered in order of severity. For each issue, the affected nodes are also listed.

Issues by Severity

2.1 - SSL/TLS: Report Weak Cipher Suites

MEDIUM: (CVSS: 5)
OID: 1.3.6.1.4.1.25623.1.0.103440
3389/TCP

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Affected Nodes
176.16.1.103, 176.16.1.115, 176.16.1.134

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA 'Weak' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA

Solution
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808) - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000) - 1024 bit RSA authentication is considered to be insecure and therefore as weak - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong

Vulnerability Detection Method
Details:SSL/TLS: Report Weak Cipher Suites(OID: 1.3.6.1.4.1.25623.1.0.103440)Version used: 2021-12-01T13:10:37+0000

References
https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html, https://bettercrypto.org/, https://mozilla.github.io/server-side-tls/ssl-config-generator/

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

MEDIUM: (CVSS: 4.3)
OID: 1.3.6.1.4.1.25623.1.0.117274
3389/TCP

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

Affected Nodes
176.16.1.103, 176.16.1.111, 176.16.1.115, 176.16.1.123, 176.16.1.134

Vulnerability Detection Result
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) VT.

Impact
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.

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 information.

Vulnerability Insight
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)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.Details:SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection(OID: 1.3.6.1.4.1.25623.1.0.117274)Version used: 2021-07-19T08:11:48+0000

References
https://ssl-config.mozilla.org/, https://bettercrypto.org/, https://datatracker.ietf.org/doc/rfc8996/, https://vnhacker.blogspot.com/2011/09/beast.html, https://web.archive.org/web/20201108095603/https://censys.io/blog/freak, https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

2.3 - SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

MEDIUM: (CVSS: 4)
OID: 1.3.6.1.4.1.25623.1.0.105880
3389/TCP

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Affected Nodes
176.16.1.134

Vulnerability Detection Result
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: CN=WGWIN7-1 Signature Algorithm: sha1WithRSAEncryption

Solution
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use: - Secure Hash Algorithm 1 (SHA-1) - Message Digest 5 (MD5) - Message Digest 4 (MD4) - Message Digest 2 (MD2) Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates. NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive: Fingerprint1 or fingerprint1, Fingerprint2

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.Details:SSL/TLS: Certificate Signed Using A Weak Signature Algorithm(OID: 1.3.6.1.4.1.25623.1.0.105880)Version used: 2021-10-15T11:13:32+0000

References
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

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

MEDIUM: (CVSS: 4)
OID: 1.3.6.1.4.1.25623.1.0.106223

3389/TCP

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

Affected Nodes
176.16.1.103, 176.16.1.115, 176.16.1.134

Vulnerability Detection Result
Server Temporary Key Size: 1024 bits

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

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.

Vulnerability Insight
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.

Vulnerability Detection Method
Checks the DHE temporary public key size.Details:SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerab...(OID: 1.3.6.1.4.1.25623.1.0.106223)Version used: 2021-02-12T06:42:15+0000

References
https://weakdh.org/, https://weakdh.org/sysadmin.html

2.5 - TCP timestamps

L

LOW: (CVSS: 2.6)

OID: 1.3.6.1.4.1.25623.1.0.80091

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

Affected Nodes
176.16.1.103, 176.16.1.115, 176.16.1.134

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 22398251 Packet 2: 22398356
Multiple results by host

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

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.

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

Vulnerability Detection Method
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.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10+0000

References
http://www.ietf.org/rfc/rfc1323.txt, http://www.ietf.org/rfc/rfc7323.txt,
https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152