YourIT!
Your Logo Goes Here

Security Assessment

External Vulnerability Scan Detail by Issue Report

Scan Date: 2021/01/19

Prepared for: Your Customer / Prospect

Prepared by: Your Company Name

2021/02/03

Table of Contents

01 Summary

02 Details

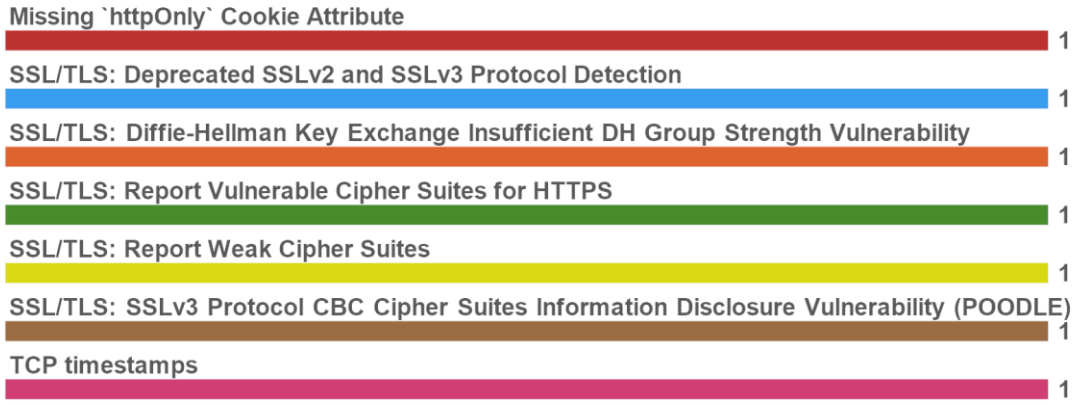
2.1 SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
2.2 Missing `httpOnly` Cookie Attribute
2.3 SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)
2.4 SSL/TLS: Report Weak Cipher Suites
2.5 SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
2.6 SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
2.7 TCP timestamps

1 - Summary

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

Issues by Severity

Issues by NVT



ISSUE	COUNT
TCP timestamps	1
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	1
SSL/TLS: Report Weak Cipher Suites	1
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	1
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	1
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	1
Missing `httpOnly` Cookie Attribute	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 Vulnerable Cipher Suites for HTTPS

MEDIUM: (CVSS: 5)
OID: 1.3.6.1.4.1.25623.1.0.108031

443/TCP (HTTPS)

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Affected Nodes
66.11.8.80(66-11-8-80.orf.contbb.net)

Vulnerability Detection Result
'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32) 'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32) 'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32) 'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Solution
The configuration of this services should be changed so that it does not accept the listed 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 vulnerable cipher suites: - 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS (OID: 1.3.6.1.4.1.25623.1.0.108031) Version used: $Revision: 5232 $

References
https://bettercrypto.org/, https://mozilla.github.io/server-side-tls/ssl-config-generator/, https://sweet32.info/

2.2 - Missing `httpOnly` Cookie Attribute

MEDIUM: (CVSS: 5)
OID: 1.3.6.1.4.1.25623.1.0.105925

80/TCP (HTTP)

Summary
The application is missing the 'httpOnly' cookie attribute

Affected Nodes
66.11.8.80(66-11-8-80.orf.contbb.net)

Vulnerability Detection Result
The cookies: Set-Cookie: FGTServer=5C75B8A34CCAA36BD5840185F53A10AC3DCECFEA75408A8CA181AECAAED019C6A17F7F9F18A6FFC41000D495C2EE; Version=***replaced***; Max-Age=3600 are missing the "httpOnly" attribute.

Solution
Set the 'httpOnly' attribute for any session cookie.

Vulnerability Insight
The flaw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Vulnerability Detection Method
Check all cookies sent by the application for a missing 'httpOnly' attribute Details: Missing `httpOnly` Cookie Attribute (OID: 1.3.6.1.4.1.25623.1.0.105925) Version used: $Revision: 5270 $

References
https://www.owasp.org/index.php/HttpOnly, https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)

2.3 - SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

MEDIUM: (CVSS: 4.3)
OID: 1.3.6.1.4.1.25623.1.0.802087

443/TCP (HTTPS)

Summary
This host is prone to an information disclosure vulnerability.

Affected Nodes
66.11.8.80(66-11-8-80.orf.contbb.net)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

Solution
Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

Vulnerability Insight
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method
Evaluate previous collected information about this service. Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.802087) Version used: $Revision: 11402 $

References
https://www.openssl.org/~bodo/ssl-poodle.pdf, https://www.imperialviolet.org/2014/10/14/poodle.html,

https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html, http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

2.4 - SSL/TLS: Report Weak Cipher Suites

M

MEDIUM: (CVSS: 4.3)

OID: 1.3.6.1.4.1.25623.1.0.103440

443/TCP (HTTPS)

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
66.11.8.80(66-11-8-80.orf.contbb.net)

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the SSLv3 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA '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: $Revision: 11135 $

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/

2.5 - SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

M

MEDIUM: (CVSS: 4.3)

OID: 1.3.6.1.4.1.25623.1.0.111012

443/TCP (HTTPS)

Summary
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Affected Nodes
66.11.8.80(66-11-8-80.orf.contbb.net)

Vulnerability Detection Result
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.802067) NVT.

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.

Solution
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

Vulnerability Insight
The SSLv2 and SSLv3 protocols containing known cryptographic flaws like: - Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566) - Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)

Vulnerability Detection Method
Check the used protocols of the services provided by this system. Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012) Version used: $Revision: 5547 $

References
https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, https://bettercrypto.org/, https://mozilla.github.io/server-side-tls/ssl-config-generator/, https://drownattack.com/, https://www.imperialviolet.org/2014/10/14/poodle.html

2.6 - 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

443/TCP (HTTPS)

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

Affected Nodes
66.11.8.80(66-11-8-80.orf.contbb.net)

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: $Revision: 12865 $

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

2.7 - 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
66.11.8.80(66-11-8-80.orf.contbb.net)

Vulnerability Detection Result
It was detected that the host implements RFC1323.

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 also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

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

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: $Revision: 10411 $

References
http://www.ietf.org/rfc/rfc1323.txt