THE CASSID GROUP
Simple. Solutions.

External Vulnerability Scan Detail Report

Scan Date: XX/XX/2018

Prepared for:
Customer
Prepared by:
The Cassid Group

XX/XX/2018

Table of Contents

1 - Summary

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to mitigate these threats.
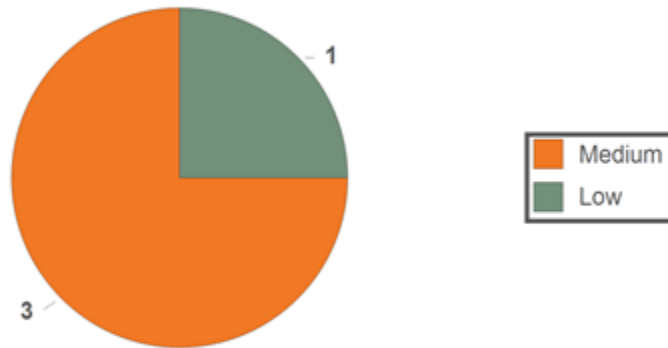
Host Issue Summary

Host	Open Ports	High	Med	Low	False	
22.33.44.55 (22-33-44-55-static.hfc.comcastbusiness.net)	2	0	3	1	0	4.3
: 1	2	0	3	1	0	4.3

Issues by NVT

NVT	Count
TCP timestamps	1
POODLE SSLv3 Protoco...	1
Deprecated SSLv2 and...	1
Check for SSL Weak C...	1

2 - Scan Details

Issues by Severity

Severity	Count
High	0
Medium	3
Low	1
False Positive	0
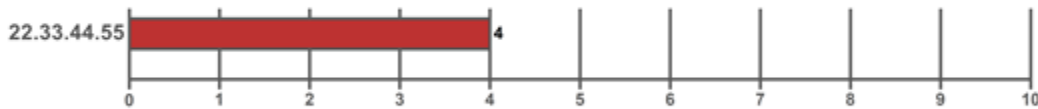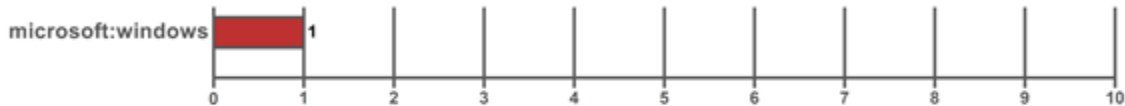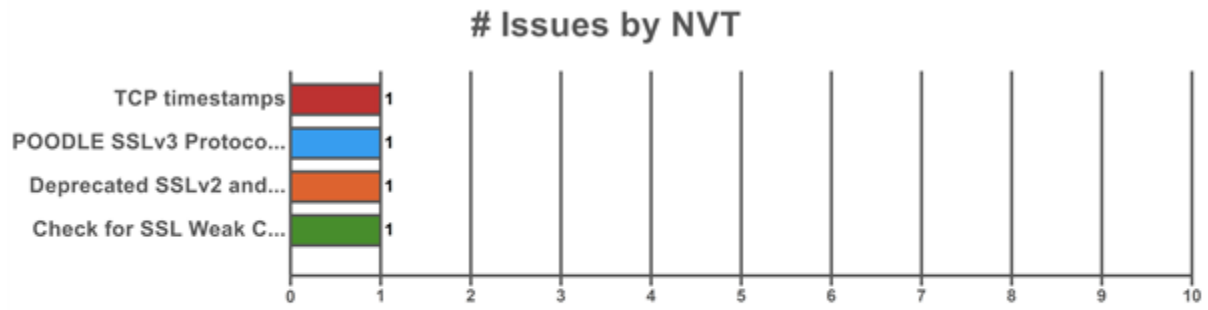
2.1 - 22.33.44.55 (22-33-44-55-static.hfc.comcastbusiness.net)

Host Issue Summary

Host	Open Ports	High	Med	Low	False	Highest CVSS
22.33.44.55 (22-33-44-55-static.hfc.comcastbusiness.net)	2	0	3	1	0	4.3

Listening Ports

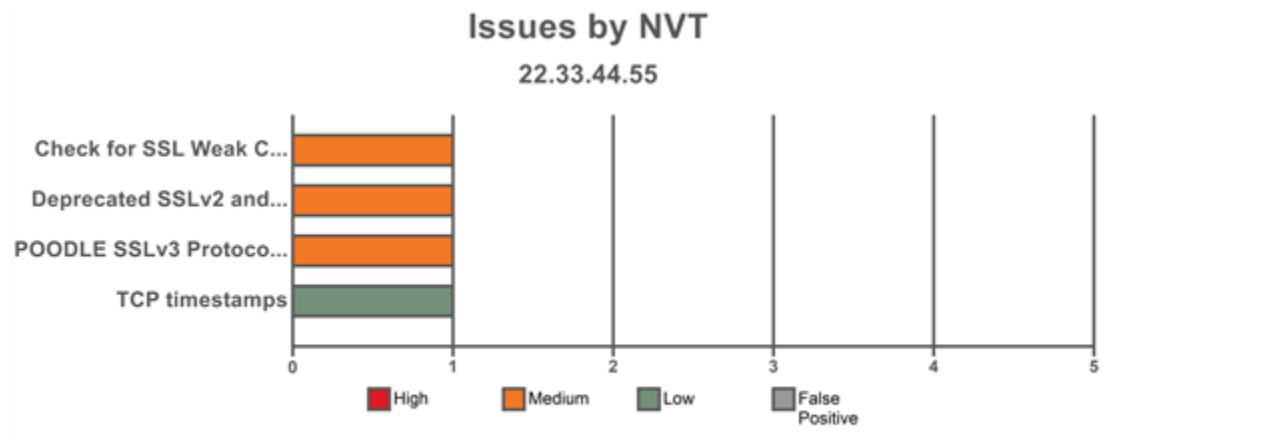| Port |
|---|
| 443/tcp (https), 1723/tcp |

NVT Issues Summary

Host	Open Ports	High	Med	Low	False	Highest CVSS
Check for SSL Weak Ciphers	443/tcp (https)	0	1	0	0	4.3
Deprecated SSLv2 and SSLv3 Protocol Detection	443/tcp (https)	0	1	0	0	4.3
POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability	443/tcp (https)	0	1	0	0	4.3
TCP timestamps		0	0	1	0	2.6

Security Issues

M	**Medium** (CVSS: 4.3) **NVT:** Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)	443/tcp (https)

Summary

This routine search for weak SSL ciphers offered by a service.

Vulnerability Detection Result

Weak ciphers offered by this service: SSL3_RSA_RC4_128_MD5   SSL3_RSA_RC4_128_SHA
TLS1_RSA_RC4_128_MD5   TLS1_RSA_RC4_128_SHA   TLS1_RSA_RC4_128_MD5
TLS1_RSA_RC4_128_SHA

Solution

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength: - Any SSL/TLS using no cipher is considered weak. - All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol. - RC4 is considered to be weak. - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods   and therefore considered as weak. - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks - 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: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440) Version used: $Revision: 3061 $

	Medium (CVSS: 4.3) **NVT:** Deprecated SSLv2 and SSLv3 Protocol Detection (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.

Vulnerability Detection Result

In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'Check SSL Weak Ciphers and Supported Ciphers' 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.

Vulnerability Detection Method

Check the used protocols of the services   provided by this system. Details: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012) Version used: $Revision: 2699 $

References

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, https://bettercrypto.org/

	Medium (CVSS: 4.3) **NVT:** POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802087)	443/tcp (https)

Summary

This host is installed with OpenSSL   and is prone to information disclosure vulnerability.

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.   Impact Level: Application

Solution

Vendor released a patch to address this   vulnerabiliy, For updates contact vendor or refer to https://www.openssl.org NOTE: The only correct way to fix POODLE is to disable SSL v3.0

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

Send a SSLv3 request and check the   response. Details: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802087) Version used: $Revision: 2752 $

References

http://osvdb.com/113251, 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

| L | **Low** (CVSS: 2.6) **NVT:** TCP timestamps (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.

Vulnerability Detection Result

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 227599908 Paket 2: 227600029

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: 3351 $

References

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