YourIT!
Your Logo Goes Here

Security Assessment

EXTERNAL NETWORK VULNERABILITIES SUMMARY

CONFIDENTIALITY NOTE: The information contained in this report is for the exclusive use of the client specified above and may contain confidential, privileged, and non-disclosable information. If you are not the client or addressee, you are strictly prohibited from reading, photocopying, distributing, or otherwise using this report or its contents in any way.

Scan Date: 2021/01/19

Prepared for: Your Customer / Prospect

Prepared by: Your Company Name

2021/02/03

External Network Vulnerabilities Summary

This report ranks individual issues based upon their CVSS while providing guidance on which issues to address by priority. To mitigate global risk and improve the health of the network, address issues with higher CVSS first.

Medium Risk

CVSS	RECOMMENDATION

5 **SSL/TLS: Report Vulnerable Cipher Suites for HTTPS**

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

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.

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

---

5 **Missing `httpOnly` Cookie Attribute**

Summary
The application is missing the 'httpOnly' cookie attribute

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

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

4.3 **SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)**

Summary
This host is prone to an information disclosure vulnerability.

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

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

4.3 **SSL/TLS: Report Weak Cipher Suites**

Summary

CVSS	RECOMMENDATION

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.

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.

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

4.3 SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

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

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.

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

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

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

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.

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

Low Risk

CVSS	RECOMMENDATION

2.6 TCP timestamps

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

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to

PROPRIETARY & CONFIDENTIAL

CVSS	RECOMMENDATION

/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

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