



Security Assessment

EXTERNAL NETWORK VULNERABILITIES SUMMARY REPORT



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

Prepared for:
Your Customer / Prospect
Prepared by:
Your Company Name

Management Plan

The Management Plan ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the global Risk Score, but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

Medium Risk

CVSS	Recommendation
4.3	<p>Check for SSL Weak Ciphers</p> <p>Summary This routine search for weak SSL ciphers offered by a service.</p> <p>Solution The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.</p> <p>Affected Nodes 22.33.44.55(22-33-44-55-static.hfc.comcastbusiness.net)</p>
4.3	<p>Deprecated SSLv2 and SSLv3 Protocol Detection</p> <p>Summary It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.</p> <p>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.</p> <p>Affected Nodes 22.33.44.55(22-33-44-55-static.hfc.comcastbusiness.net)</p>
4.3	<p>POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability</p> <p>Summary This host is installed with OpenSSL and is prone to information disclosure vulnerability.</p> <p>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</p> <p>Affected Nodes 22.33.44.55(22-33-44-55-static.hfc.comcastbusiness.net)</p>

Low Risk

CVSS	Recommendation
2.6	<p data-bbox="328 262 537 321">TCP timestamps Summary</p> <p data-bbox="328 321 1393 352">The remote host implements TCP timestamps and therefore allows to compute the uptime.</p> <p data-bbox="328 384 435 415">Solution</p> <p data-bbox="328 415 1419 657">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</p> <p data-bbox="328 688 521 720">Affected Nodes</p> <p data-bbox="328 720 1000 751">22.33.44.55(22-33-44-55-static.hfc.comcastbusiness.net)</p>