Strategic Intent Consulting Group
An Information Technology Innovation Company

Security Assessment

EXTERNAL NETWORK VULNERABILITIES SUMMARY REPORT

Prepared for: ABC Company

Prepared by: Strategic Intent Consulting Group, Inc.

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	**Check for SSL Weak Ciphers** **Summary** This routine search for weak SSL ciphers offered by a service. **Solution** The configuration of this services should be changed so that it does not support the listed weak ciphers anymore. **Affected Nodes** 22.33.44.55(22-33-44-55-static.hfc.comcastbusiness.net)
4.3	**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** 22.33.44.55(22-33-44-55-static.hfc.comcastbusiness.net)
4.3	**POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability** **Summary** This host is installed with OpenSSL and is prone to information disclosure vulnerability. **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 **Affected Nodes** 22.33.44.55(22-33-44-55-static.hfc.comcastbusiness.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 /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** 22.33.44.55(22-33-44-55-static.hfc.comcastbusiness.net)