Security Assessment

Vulnerability Management Plan

Prepared for: Your Company
Prepared by: Dave at eSOZO Computer & Network Services

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.

High Risk

CVSS	Recommendation
8.5	**OpenSSH Multiple Vulnerabilities** **Summary** This host is running OpenSSH and is prone to multiple vulnerabilities. **Solution** Upgrade to OpenSSH 7.0 or later. For updates refer to http://www.openssh.com **Affected Nodes** 12.34.56.78 (static-87.56.43.21.name.isp.com)
7.2	**OpenSSH Privilege Escalation Vulnerability - May16** **Summary** This host is installed with openssh and is prone to privilege escalation vulnerability. **Solution** Upgrade to OpenSSH version 7.2p2-3 or later. For updates refer to http://www.openssh.com **Affected Nodes** 12.34.56.78 (static-87.56.43.21.name.isp.com)

Medium Risk

CVSS	Recommendation
6.8	**OpenSSL CCS Man in the Middle Security Bypass Vulnerability** **Summary** OpenSSL is prone to security-bypass vulnerability. **Solution** Updates are available. **Affected Nodes** 12.34.56.78 (static-87.56.43.21.name.isp.com)
6.5	**OpenSSH Client Information Leak** **Summary** The OpenSSH client code between 5.4 and 7.1 contains experimental support for resuming SSH-connections (roaming). The matching server code has never been shipped, but the client code was enabled by default and could be tricked by a malicious server into leaking client memory to the server, including private client user keys. The authentication of the server host key prevents exploitation by a man-in-the-middle, so this information leak is restricted to connections to malicious or compromised servers. **Solution** Update to 7.1p or newer. **Affected Nodes** 12.34.56.78 (static-87.56.43.21.name.isp.com)
6.4	**Microsoft RDP Server Private Key Information Disclosure Vulnerability** **Summary** This host is running Remote Desktop Protocol server and is prone to information disclosure vulnerability. **Solution** No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one. A workaround is to connect only to terminal services over trusted networks. **Affected Nodes** 12.34.56.78 (static-87.56.43.21.name.isp.com)
5.8	**IIS Possible Compromise** **Summary** One or more files were found on this host that indicate a possible compromise. **Solution** Investigate the discovered files **Affected Nodes** 12.34.56.78 (static-87.56.43.21.name.isp.com)

5.5	**OpenSSH <= 7.2p1 - Xauth Injection** **Summary** openssh xauth command injection may lead to forced-command and /bin/false bypass **Solution** Upgrade to OpenSSH version 7.2p2 or later. For updates refer to http://www.openssh.com **Affected Nodes** 12.34.56.78 (static-87.56.43.21.name.isp.com)
5	**Netware Web Server Sample Page Source Disclosure** **Summary** On a Netware Web Server, viewcode.jse allows the source code of web pages to be viewed. As an argument, a URL is passed to sewse.nlm. The URL can be altered and will permit files outside of the web root to be viewed. As a result, sensitive information could be obtained from the Netware server, such as the RCONSOLE password located in AUTOEXEC.NCF. Example: http://target//lcgi/sewse.nlm?sys:/novonyx/suitespot/docs/sewse/viewcode.jse+httplist+httplist/../../../../../system/autoexec.ncf **Solution** Remove sample NLMs and default files from the web server. Also, ensure the RCONSOLE password is encrypted and utilize a password protected screensaver for console access. **Affected Nodes** 12.34.56.78 (static-87.56.43.21.name.isp.com)
5	**OpenSSH Denial of Service Vulnerability - Jan16** **Summary** This host is installed with openssh and is prone to denial of service vulnerability. **Solution** Upgrade to OpenSSH version 7.1p2 or later. For updates refer to http://www.openssh.com **Affected Nodes** 12.34.56.78 (static-87.56.43.21.name.isp.com)
4.3	**Joomla! Currency Converter Module from Parameter Cross-Site Scripting Vulnerability** **Summary** This host is running Joomla with Currency Converter module and is prone to cross-site scripting vulnerability. **Solution** No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one. **Affected Nodes** 12.34.56.78 (static-87.56.43.21.name.isp.com)

4.3	**Check for SSL Weak Ciphers** **Summary** This routine search for weak SSL ciphers offered by a service. **Solution** The configuration of these services should be changed so that it does not support the listed weak ciphers anymore. **Affected Nodes** 12.34.56.78 (static-87.56.43.21.name.isp.com)
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 vulnerability, 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** 12.34.56.78 (static-87.56.43.21.name.isp.com)
4.3	**i-Gallery d Parameter Cross Site Scripting Vulnerability** **Summary** i-Gallery is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. An attacker could leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This could allow the attacker to steal cookie-based authentication credentials and launch other attacks. I-Gallery 3.4 is vulnerable other versions may also be affected. **Solution** **Affected Nodes** 12.34.56.78 (static-87.56.43.21.name.isp.com)
4.3	**SSH Weak Encryption Algorithms Supported** **Summary** The remote SSH server is configured to allow weak encryption algorithms. **Solution** Disable the weak encryption algorithms. **Affected Nodes** 12.34.56.78 (static-87.56.43.21.name.isp.com)

4.3	**OpenSSH Security Bypass Vulnerability** **Summary** This host is running OpenSSH and is prone to security bypass vulnerability. **Solution** Upgrade to OpenSSH version 6.9 or later. For updates refer to http://www.openssh.com **Affected Nodes** 12.34.56.78 (static-87.56.43.21.name.isp.com)
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** 12.34.56.78 (static-87.56.43.21.name.isp.com)

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 cannot 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** 12.34.56.78 (static-87.56.43.21.name.isp.com)
2.6	**SSH Weak MAC Algorithms Supported** **Summary** The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms. **Solution** Disable the weak MAC algorithms. **Affected Nodes** 12.34.56.78 (static-87.56.43.21.name.isp.com)
2.6	**Private IP address leaked in HTTP headers** **Summary** This web server leaks a private IP address through its HTTP headers. **Solution** See the references for possible workarounds and updates. **Affected Nodes** 12.34.56.78 (static-87.56.43.21.name.isp.com)