YourIT!
Your Logo Goes Here

Security Assessment

INTERNAL NETWORK VULNERABILITIES SUMMARY REPORT

Scan Date: 10/25/2016

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

10/27/2016

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
10	**MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check)** **Summary** This host is missing an important security update according to Microsoft Bulletin MS15-034. **Solution** Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-034 **Affected Nodes** 192.168.1.5(VPNGW), 192.168.1.15(UTIL12), 192.168.6.159(VPNGW)
10	**PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Linux)** **Summary** This host is installed with PHP and is prone to denial of service and unspecified Vulnerabilities **Solution** Upgrade to PHP version 5.5.32, or 5.6.18, or 7.0.3, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
10	**PHP type confusion Denial of Service Vulnerability (Linux)** **Summary** This host is installed with PHP and is prone to denial of service vulnerability. **Solution** Upgrade to PHP version 5.6.7 or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
10	**Samba TALLOC_FREE() Function Remote Code Execution Vulnerability** **Summary** Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability **Solution** Updates are available. Please see the references or vendor advisory for more information.

CVSS	Recommendation
	Affected Nodes 192.168.1.50(myco-bdr), 192.168.6.82(MINTLINUX)
10	**PHP End Of Life Detection (Linux)** **Summary** The PHP version on the remote host has reached the end of life and should not be used anymore. **Solution** Update the PHP version on the remote host to a still supported version. **Affected Nodes** 192.168.1.50(myco-bdr)
10	**PHP phar_fix_filepath Function Stack Buffer Overflow Vulnerability - Mar16 (Linux)** **Summary** This host is installed with PHP and is prone to stack buffer overflow vulnerability. **Solution** Upgrade to PHP version 5.4.43, or 5.5.27, or 5.6.11 or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
10	**NFS export** **Summary** This plugin lists NFS exported shares, and warns if some of them are readable. It also warns if the remote NFS server is superfluous. Tested on Ubuntu/Debian mountd **Solution** **Affected Nodes** 192.168.1.50(myco-bdr)
10	**VMSA-2015-0007: VMware ESXi OpenSLP Remote Code Execution (remote check)** **Summary** VMware vCenter and ESXi updates address critical security issues. **Solution** Apply the missing patch(es). **Affected Nodes** 192.168.6.154
10	**Discard port open** **Summary** The remote host is running a 'discard' service. This service typically sets up a listening socket and will ignore all the data which it receives. This service is unused these days, so it is

CVSS	Recommendation
	advised that you disable it. **Solution** - Under Unix systems, comment out the 'discard' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry key to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDiscard Then launch cmd.exe and type : net stop simptcp net start simptcp To restart the service. **Affected Nodes** 192.168.7.68(REMOTE)
10	**Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)** **Summary** This host is missing a critical security update according to Microsoft Bulletin MS10-012. **Solution** Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx **Affected Nodes** 192.168.7.68(REMOTE)
10	**ProFTPD `mod_copy` Unauthenticated Copying Of Files Via SITE CPFR/CPTO** **Summary** ProFTPD is prone to an unauthenticated copying of files vulnerability. **Solution** Ask the vendor for an update **Affected Nodes** 192.168.1.50(myco-bdr)
10	**Trojan horses** **Summary** An unknown service runs on this port. It is sometimes opened by Trojan horses. Unless you know for sure what is behind it, you'd better check your system. **Solution** if a trojan horse is running, run a good antivirus scanner **Affected Nodes** 192.168.6.14(Psolidad-WIN764), 192.168.6.30(Mwest-WIN864), 192.168.7.68(REMOTE)
10	**IPMI Cipher Zero Authentication Bypass Vulnerability** **Summary** Intelligent Platform Management Interface is prone to an authentication- bypass vulnerability. **Solution** Ask the Vendor for an update. **Affected Nodes**

CVSS	Recommendation
	192.168.1.201, 192.168.1.202, 192.168.1.203, 192.168.1.204, 192.168.1.205
9.3	**Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387)** **Summary** This host is missing a critical security update according to Microsoft Bulletin MS12-020. **Solution** Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://technet.microsoft.com/en-us/security/bulletin/ms12-020 **Affected Nodes** 192.168.7.68(REMOTE)
9	**SSH Brute Force Logins with default Credentials** **Summary** A number of known default credentials is tried for log in via SSH protocol. **Solution** Change the password as soon as possible. **Affected Nodes** 192.168.1.1, 192.168.5.1
8.5	**Microsoft SQL Server Multiple Vulnerabilities (3065718) - Remote** **Summary** This host is missing an important security update according to Microsoft Bulletin MS15-058. **Solution** Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from this link, https://technet.microsoft.com/library/security/MS15-058 **Affected Nodes** 192.168.1.16(sourcesvr)
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** 192.168.0.3, 192.168.1.24, 192.168.1.203, 192.168.1.204, 192.168.1.205, 192.168.6.82(MINTLINUX)
7.8	**OpenSSH auth_password Denial of Service Vulnerability (Linux)** **Summary** This host is installed with openssh and is prone to denial of service vulnerability. **Solution**

CVSS	Recommendation
	Upgrade to OpenSSH version 7.3 or later. For updates refer to http://www.openssh.com **Affected Nodes** 192.168.1.24, 192.168.1.201, 192.168.1.202, 192.168.1.203, 192.168.1.204, 192.168.1.205, 192.168.6.82(MINTLINUX)
7.5	**PHP Multiple Double Free Vulnerabilities - Jan15** **Summary** This host is installed with PHP and is prone to denial of service vulnerability. **Solution** Upgrade to PHP version 5.5.21 or 5.6.5 or later **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP Remote Code Execution and Denial of Service Vulnerabilities - Dec13** **Summary** This host is installed with PHP and is prone to remote code execution vulnerability. **Solution** Update to PHP version 5.3.28 or 5.4.23 or 5.5.7 or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP Out of Bounds Read Multiple Vulnerabilities - Jan15** **Summary** This host is installed with PHP and is prone to denial of service vulnerability. **Solution** Upgrade to PHP version 5.4.37 or 5.5.21 or 5.6.5 or later **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP Multiple Vulnerabilities - 02 - Jan15** **Summary** This host is installed with PHP and is prone to multiple vulnerbilities. **Solution** Upgrade to PHP version 5.6.5 or later **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**Lighttpd Multiple vulnerabilities** **Summary** This host is running Lighttpd and is prone to multiple vulnerabilities

CVSS	Recommendation
	Solution Upgrade to 1.4.35 or higher, For updates refer to http://www.lighttpd.net/download **Affected Nodes** 192.168.0.241, 192.168.1.240
7.5	**Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability** **Summary** The host is running SMB/NETBIOS and prone to authentication bypass 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, - Disable null session login. - Remove the share. - Enable passwords on the share. **Affected Nodes** 192.168.1.31(HVFS), 192.168.1.32(HVFS), 192.168.1.33(HVFS), 192.168.1.34(HVFS)
7.5	**Report default community names of the SNMP Agent** **Summary** Simple redi Management Protocol (SNMP) is a protocol which can be used by administrators to remotely manage a computer or redi device. There are typically 2 modes of remote SNMP monitoring. These modes are roughly 'READ' and 'WRITE' (or PUBLIC and PRIVATE). **Solution** Determine if the detected community string is a private community string. Determine whether a public community string exposes sensitive information. Disable the SNMP service if you don't use it or change the default community string. **Affected Nodes** 192.168.0.2, 192.168.0.11, 192.168.1.24, 192.168.1.205
7.5	**OpenSSH schnorr.c Remote Memory Corruption Vulnerability** **Summary** OpenSSH is prone to a remote memory-corruption vulnerability. **Solution** Updates are available. **Affected Nodes** 192.168.0.3, 192.168.1.203, 192.168.1.204, 192.168.1.205
7.5	**PHP Multiple Vulnerabilities - 01 - Mar16 (Linux)** **Summary** This host is installed with PHP and is prone to multiple vulnerabilities. **Solution** Upgrade to PHP version 5.4.44 or 5.5.28 or 5.6.12 or later. For updates refer to http://www.php.net

CVSS	Recommendation
	Affected Nodes 192.168.1.50(myco-bdr)
7.5	**PHP Multiple Vulnerabilities - 04 - Aug16 (Linux)** **Summary** This host is installed with PHP and is prone to multiple vulnerabilities. **Solution** Upgrade to PHP version 5.5.36, or 5.6.22, or 7.0.7, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP Multiple Vulnerabilities - 03 - Sep16 (Linux)** **Summary** This host is installed with PHP and is prone to multiple vulnerabilities. **Solution** Upgrade to PHP version 5.6.25, or 7.0.10, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP Multiple Vulnerabilities - 02 - Aug16 (Linux)** **Summary** This host is installed with PHP and is prone to multiple vulnerabilities. **Solution** Upgrade to PHP version 5.5.37, or 5.6.23, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP Multiple Vulnerabilities - 03 - Aug16 (Linux)** **Summary** This host is installed with PHP and is prone to multiple vulnerabilities. **Solution** Upgrade to PHP version 5.5.36, or 5.6.22, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP Multiple Vulnerabilities - 02 - Sep16 (Linux)** **Summary** This host is installed with PHP and is prone to multiple vulnerabilities. **Solution** Upgrade to PHP version 5.6.25, or 7.0.10, or later. For updates refer to http://www.php.net

CVSS	Recommendation
	Affected Nodes 192.168.1.50(myco-bdr)
7.5	**APC redi Management Card Telnet Default Credentials** **Summary** The remote APC redi Management Card has default credentials set. **Solution** Change/Set the password. **Affected Nodes** 192.168.1.52
7.5	**APC redi Management Card Webinterface Default Credentials** **Summary** The remote APC redi Management Card Webinterface is prone to a default account authentication bypass vulnerability. **Solution** Change the password. **Affected Nodes** 192.168.1.52
7.5	**PHP var_unserializer Denial of Service Vulnerability (Linux)** **Summary** This host is installed with PHP and is prone to denial of service vulnerability. **Solution** Upgrade to PHP version 5.6.26, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP libgd Denial of Service Vulnerability (Linux)** **Summary** This host is installed with PHP and is prone to denial of service vulnerability. **Solution** The patch is available from the below link https://github.com/php/php-src/pull/2119 For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP Multiple Vulnerabilities - 01 - Aug16 (Linux)** **Summary** This host is installed with PHP and is prone to multiple vulnerabilities. **Solution** Upgrade to PHP version 5.5.37, or 5.6.23, or 7.0.8, or later. For updates refer to

CVSS	Recommendation
	http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP Multiple Vulnerabilities - 01 - Jul16 (Linux)** **Summary** This host is installed with PHP and is prone to multiple vulnerabilities. **Solution** Upgrade to PHP version 5.5.34, or 5.6.20, or 7.0.5, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP Multiple Vulnerabilities - 03 - Jul16 (Linux)** **Summary** This host is installed with PHP and is prone to multiple vulnerabilities. **Solution** Upgrade to PHP version 5.5.35, or 5.6.21, or 7.0.6, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP serialize_function_call Function Type Confusion Vulnerability - Mar16 (Linux)** **Summary** This host is installed with PHP and is prone to remote code execution vulnerability. **Solution** Upgrade to PHP version 5.4.45, or 5.5.29, or 5.6.13 or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP Multiple Vulnerabilities - 01 - Apr16 (Linux)** **Summary** This host is installed with PHP and is prone to multiple vulnerabilities. **Solution** Upgrade to PHP version 5.5.33 or 5.6.19 or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP Multiple Vulnerabilities - 04 - Jul16 (Linux)** **Summary** This host is installed with PHP and is prone to multiple vulnerabilities.

CVSS	Recommendation
	Solution Upgrade to PHP version 5.4.44, or 5.5.28, or 5.6.12, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP Multiple Vulnerabilities - 05 - Aug16 (Linux)** **Summary** This host is installed with PHP and is prone to multiple vulnerabilities. **Solution** Upgrade to PHP version 5.4.42, or 5.5.26, or 5.6.10, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP Arbitrary Code Execution Vulnerability - Aug16 (Linux)** **Summary** This host is installed with PHP and is prone to arbitrary code execution vulnerability **Solution** Upgrade to PHP version 5.5.27, or 5.6.11, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP Multiple Vulnerabilities - 05 - Jul16 (Linux)** **Summary** This host is installed with PHP and is prone to multiple vulnerabilities. **Solution** Upgrade to PHP version 5.5.38, or 5.6.24, or 7.0.9, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
7.5	**PHP Directory Traversal Vulnerability - Jul16 (Linux)** **Summary** This host is installed with PHP and is prone to Directory traversal vulnerability. **Solution** Upgrade to PHP version 5.4.45, or 5.5.29, or 5.6.13, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)

CVSS	Recommendation
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** 192.168.0.3, 192.168.1.24, 192.168.1.201, 192.168.1.202, 192.168.1.203, 192.168.1.204, 192.168.1.205, 192.168.6.82(MINTLINUX)
7.1	**PHP Denial of Service Vulnerability - 01 - Jul16 (Linux)** **Summary** This host is installed with PHP and is prone to denial of service vulnerability. **Solution** Upgrade to PHP version 5.5.28, or 5.6.12, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)

Medium Risk

CVSS	Recommendation
6.9	**OpenSSH X Connections Session Hijacking Vulnerability** **Summary** OpenSSH is prone to a vulnerability that allows attackers to hijack forwarded X connections. Successfully exploiting this issue may allow an attacker run arbitrary shell seq with the privileges of the acct running the affected application. This issue affects OpenSSH 4.3p2 other versions may also be affected. NOTE: This issue affects the portable version of OpenSSH and may not affect OpenSSH running on OpenBSD. **Solution** Updates are available. Please see the references for more information. **Affected Nodes** 192.168.0.3
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** 192.168.1.240, 192.168.6.49
6.8	**OpenSSL DSA_verify() Security Bypass Vulnerability in BIND** **Summary**

CVSS	Recommendation
	The host is running BIND and is prone to Security Bypass Vulnerability. **Solution** Upgrade to version 9.6.0 P1, 9.5.1 P1, 9.4.3 P1, 9.3.6 P1 https://www.isc.org/downloadables/11 **Affected Nodes** 192.168.3.2
6.8	**Microsoft SQL Server Elevation of Privilege Vulnerability (2984340) - Remote** **Summary** This host is missing an important security update according to Microsoft Bulletin MS14-044. **Solution** Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from this link, https://technet.microsoft.com/library/security/MS14-044 **Affected Nodes** 192.168.1.16(sourcesvr), 192.168.7.99(PS01)
6.8	**PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux)** **Summary** This host is installed with PHP and is prone to denial of service and unspecified Vulnerabilities **Solution** Upgrade to PHP version 5.6.18, or 7.0.3, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
6.8	**PHP XML Entity Expansion And XML External Entity Vulnerabilities (Linux)** **Summary** This host is installed with PHP and is prone to XML entity expansion and XML external entity vulnerbilities **Solution** Upgrade to PHP version 5.5.22, or 5.6.6, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
6.8	**PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux)** **Summary** This host is installed with PHP and is prone to multiple denial of service vulnerabilities. **Solution** Upgrade to PHP 5.5.30 or 5.6.14 or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)

CVSS	Recommendation
6.8	**Samba libcli/smb/smbXcli_base.c Man In The Middle (MIMA) Vulnerability** **Summary** This host is running Samba and is prone to man-in-the-middle vulnerability. **Solution** Upgrade to Samba version 4.2.14 or 4.3.11 or 4.4.5 or later. For updates refer to https://www.samba.org **Affected Nodes** 192.168.6.82(MINTLINUX)
6.8	**Samba Badlock Critical Vulnerability** **Summary** This host is running Samba and is prone to badlock vulnerability. **Solution** Upgrade to samba version 4.2.11, or 4.3.8, or 4.4.2, or later. **Affected Nodes** 192.168.1.50(myco-bdr), 192.168.6.82(MINTLINUX)
6.8	**VMSA-2016-0002: VMware product updates address a critical glibc security vulnerability (remote check)** **Summary** VMware product updates address a critical glibc security vulnerability **Solution** Apply the missing patch(es). **Affected Nodes** 192.168.6.154
6.5	**VMSA-2016-0001 VMware ESXi, Fusion, Player, and Workstation updates address important guest privilege escalation vulnerability (remote check)** **Summary** VMware ESXi, Fusion, Player, and Workstation updates address important guest privilege escalation vulnerability **Solution** Apply the missing patch(es). **Affected Nodes** 192.168.6.154
6.4	**PHP make_http_soap_request Information Disclosure Vulnerability (Linux)** **Summary** This host is installed with PHP and is prone to denial of service or information disclosure vulnerabilities **Solution** Upgrade to PHP version 5.4.44, or 5.5.28, or 5.6.12, or 7.0.4, or later. For updates refer to http://www.php.net

CVSS	Recommendation
	Affected Nodes 192.168.1.50(myco-bdr)
6.4	**Microsoft Windows SMTP Server DNS spoofing vulnerability** **Summary** The Microsoft Windows Simple Mail Transfer Protocol (SMTP) Server is prone to a DNS spoofing vulnerability. Successfully exploiting this issue allows remote attackers to spoof DNS replies, allowing them to redirect redi traffic and to launch man-in-the-middle attacks. **Solution** This issue is reported to be patched in Microsoft security advisory MS10-024 please see the references for more information. **Affected Nodes** 192.168.7.68(REMOTE)
6.4	**PHP Denial of Service Vulnerability - 02 - Aug16 (Linux)** **Summary** This host is installed with PHP and is prone to denial of service vulnerability. **Solution** Upgrade to PHP version 5.5.31, or 5.6.17, or 7.0.2, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
6.4	**PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Linux)** **Summary** This host is installed with PHP and is prone to out-of-bounds read memory corruption vulnerability. **Solution** Upgrade to PHP version 5.5.31, or 5.6.17 or 7.0.2 or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
5.8	**PHP Directory Traversal Vulnerability** **Summary** PHP is prone to a directory-traversal vulnerability because it fails to properly sanitize acct-supplied input. **Solution** Updates are available. Please see the references for more information. **Affected Nodes** 192.168.1.50(myco-bdr)

CVSS	Recommendation
5.8	**OpenSSH child_set_env() Function Security Bypass Vulnerability** **Summary** OpenSSH is prone to a security-bypass vulnerability. **Solution** Updates are available. **Affected Nodes** 192.168.0.3, 192.168.1.203, 192.168.1.204, 192.168.1.205
5.8	**OpenSSH Certificate Validation Security Bypass Vulnerability** **Summary** OpenSSH is prone to a security-bypass vulnerability. **Solution** Updates are available. **Affected Nodes** 192.168.0.3, 192.168.1.203, 192.168.1.204, 192.168.1.205
5.5	**Dropbear SSH CRLF Injection Vulnerability** **Summary** This host is installed with dropbear ssh and is prone to crlf injection vulnerability. **Solution** Upgrade to Dropbear SSH version 2016.72 or later. For updates refer to http://www.openssh.com **Affected Nodes** 192.168.0.11, 192.168.1.240, 192.168.6.49
5.5	**OpenSSH <= 7.2p1 - Xauth Injection** **Summary** openssh xauth dbre injection may lead to forced-dbre and /bin/false bypass **Solution** Upgrade to OpenSSH version 7.2p2 or later. For updates refer to http://www.openssh.com **Affected Nodes** 192.168.0.3, 192.168.1.24, 192.168.1.201, 192.168.1.202, 192.168.1.203, 192.168.1.204, 192.168.1.205, 192.168.6.82(MINTLINUX)
5.1	**PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux)** **Summary** This host is installed with PHP and is prone to Man-in-the-middle attack vulnerability. **Solution** Upgrade to PHP version 7.0.9 or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)

CVSS	Recommendation
5.1	**IPMI MD2 Auth Type Support Enabled** **Summary** IPMI MD2 auth type support is enabled on the remote host. **Solution** Disable MD2 auth type support. **Affected Nodes** 192.168.1.201, 192.168.1.202, 192.168.1.203, 192.168.1.204, 192.168.1.205
5	**SNMP GETBULK Reflected DrDoS** **Summary** The remote SNMP daemon allows distributed reflection and amplification (DrDoS) attacks **Solution** Disable the SNMP service on the remote host if you do not use it or restrict access to this service **Affected Nodes** 192.168.0.2, 192.168.1.24
5	**Use LDAP search request to retrieve information from NT Directory Services** **Summary** It is possible to disclose LDAP information. Description : The directory base of the remote server is set to NULL. This allows information to be enumerated without any prior knowledge of the directory structure. **Solution** If pre-Windows 2000 compatibility is not required, remove pre-Windows 2000 compatibility as follows : - start cmd.exe - execute the dbre : net localgroup 'Pre-Windows 2000 Compatible Access' everyone /delete - restart the remote host **Affected Nodes** 192.168.1.3(DC03), 192.168.1.4, 192.168.1.23
5	**TCP Sequence Number Approximation Reset Denial of Service Vulnerability** **Summary** The host is running TCP services and is prone to denial of service vulnerability. **Solution** Please see the referenced advisories for more information on obtaining and applying fixes. **Affected Nodes** 192.168.0.1, 192.168.0.3, 192.168.0.11, 192.168.0.241, 192.168.0.242, 192.168.1.201, 192.168.1.202, 192.168.1.203, 192.168.1.204, 192.168.1.205, 192.168.1.240, 192.168.6.49, 192.168.6.128
5	**SSL Certification Expired** **Summary** The remote server's SSL certificate has already expired. **Solution**

CVSS	Recommendation
	Replace the SSL certificate by a new one. **Affected Nodes** 192.168.1.15(UTIL12), 192.168.1.69, 192.168.1.81, 192.168.6.5, 192.168.6.142(QB01)
5	**DCE Services Enumeration** **Summary** Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. **Solution** filter incoming traffic to this port. **Affected Nodes** 192.168.1.3(DC03), 192.168.1.4, 192.168.1.5(VPNGW), 192.168.1.15(UTIL12), 192.168.1.16(sourcesvr), 192.168.1.21, 192.168.1.23, 192.168.1.31(HVFS), 192.168.1.32(HVFS), 192.168.1.33(HVFS), 192.168.1.34(HVFS), 192.168.1.41(FILE2012-1), 192.168.1.63(PITWDS12), 192.168.1.64(PITWDS12), 192.168.1.65(STORAGE12), 192.168.1.66(STORAGE12), 192.168.1.67(STORAGE12), 192.168.1.69, 192.168.1.81, 192.168.1.100(HV00), 192.168.1.104(HV04), 192.168.1.121(HV02), 192.168.1.122(HV02), 192.168.1.123(HV02), 192.168.1.254(monitor-GW), 192.168.6.5, 192.168.6.9(HPDT-8CC5260NXY), 192.168.6.10(WIN7-TEMP-1), 192.168.6.12(Psolidad-PC), 192.168.6.14(Psolidad-WIN764), 192.168.6.22, 192.168.6.26(HPLT-5CD4411D8Z), 192.168.6.30(Mwest-WIN864), 192.168.6.37(betty-INSPIRON), 192.168.6.44(b2b-GW), 192.168.6.45(DESKTOP-UAE29E6), 192.168.6.52(WILLARD), 192.168.6.56(CONFERENCE-ROOM), 192.168.6.63(buildbox), 192.168.6.67(sourcesvrBUILD), 192.168.6.68(FRONTDOOR), 192.168.6.70(WIN-888AUK4TQ2S), 192.168.6.73(WIN-D1LTOO0FR17), 192.168.6.79(Mcarrier-ASUS), 192.168.6.80(darkhorse), 192.168.6.81(Lalexander-PC), 192.168.6.86(WIN-UH2DKI2HMN4), 192.168.6.88(WIN-1OOISUH62LO), 192.168.6.100(HV04), 192.168.6.105(HV04), 192.168.6.108(HV04), 192.168.6.112(REX), 192.168.6.120(PKWIN8-VM), 192.168.6.123(HV01), 192.168.6.124(HV01), 192.168.6.125(WAMPA), 192.168.6.126(Tneusome-HP), 192.168.6.130(porchanko-HOME), 192.168.6.132(SARLACC), 192.168.6.133(PANOPTICON), 192.168.6.142(QB01), 192.168.6.151(HV01), 192.168.6.159(VPNGW), 192.168.6.161(ROWBOT), 192.168.6.165(IRIDIUM), 192.168.6.195(tarsis), 192.168.7.44(JIM-WIN8), 192.168.7.68(REMOTE), 192.168.7.95(Mmichaels-HP), 192.168.7.99(PS01), 192.168.7.123(ISTCORP-PC)
5	**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** 192.168.0.11, 192.168.0.241, 192.168.1.1, 192.168.1.3(DC03), 192.168.1.4, 192.168.1.5(VPNGW), 192.168.1.15(UTIL12), 192.168.1.16(sourcesvr), 192.168.1.21, 192.168.1.23, 192.168.1.31(HVFS), 192.168.1.32(HVFS), 192.168.1.33(HVFS), 192.168.1.34(HVFS), 192.168.1.41(FILE2012-1), 192.168.1.63(PITWDS12),

CVSS	Recommendation
	192.168.1.64(PITWDS12), 192.168.1.65(STORAGE12), 192.168.1.66(STORAGE12), 192.168.1.67(STORAGE12), 192.168.1.69, 192.168.1.81, 192.168.1.100(HV00), 192.168.1.104(HV04), 192.168.1.121(HV02), 192.168.1.122(HV02), 192.168.1.123(HV02), 192.168.1.201, 192.168.1.202, 192.168.1.203, 192.168.1.204, 192.168.1.205, 192.168.1.240, 192.168.5.1, 192.168.6.5, 192.168.6.7, 192.168.6.9(HPDT-8CC5260NXY), 192.168.6.10(WIN7-TEMP-1), 192.168.6.11, 192.168.6.12(Psolidad-PC), 192.168.6.14(Psolidad-WIN764), 192.168.6.16(svr1-65LI), 192.168.6.21(svr1-99ZO), 192.168.6.22, 192.168.6.26(HPLT-5CD4411D8Z), 192.168.6.30(Mwest-WIN864), 192.168.6.37(betty-INSPIRON), 192.168.6.44(b2b-GW), 192.168.6.45(DESKTOP-UAE29E6), 192.168.6.47, 192.168.6.48(svr1-99ZP), 192.168.6.49, 192.168.6.52(WILLARD), 192.168.6.56(CONFERENCE-ROOM), 192.168.6.57(svr1-99ZW), 192.168.6.63(buildbox), 192.168.6.67(sourcesvrBUILD), 192.168.6.70(WIN-888AUK4TQ2S), 192.168.6.73(WIN-D1LTOO0FR17), 192.168.6.80(darkhorse), 192.168.6.81(Lalexander-PC), 192.168.6.86(WIN-UH2DKI2HMN4), 192.168.6.87(svr1-91OD), 192.168.6.88(WIN-1OOISUH62LO), 192.168.6.92, 192.168.6.96, 192.168.6.100(HV04), 192.168.6.105(HV04), 192.168.6.107(svr1-99ZB), 192.168.6.108(HV04), 192.168.6.112(REX), 192.168.6.120(PKWIN8-VM), 192.168.6.123(HV01), 192.168.6.124(HV01), 192.168.6.125(WAMPA), 192.168.6.126(Tneusome-HP), 192.168.6.130(porchanko-HOME), 192.168.6.132(SARLACC), 192.168.6.133(PANOPTICON), 192.168.6.142(QB01), 192.168.6.150(workstation-TEST1), 192.168.6.151(HV01), 192.168.6.154, 192.168.6.159(VPNGW), 192.168.6.161(ROWBOT), 192.168.6.195(tarsis), 192.168.7.44(JIM-WIN8), 192.168.7.95(Mmichaels-HP), 192.168.7.99(PS01), 192.168.7.123(ISTCORP-PC)
5	**LDAP allows null bases** **Summary** It is possible to disclose LDAP information. Description : Improperly configured LDAP servers will allow the directory BASE to be set to NULL. This allows information to be culled without any prior knowledge of the directory structure. Coupled with a NULL BIND, an anonymous acct can query your LDAP server using a tool such as 'LdapMiner' **Solution** Disable NULL BASE queries on your LDAP server **Affected Nodes** 192.168.1.3(DC03), 192.168.1.4, 192.168.1.23
5	**Lighttpd http_auth.c Remote Code Execution Vulnerability - June15 (Linux)** **Summary** This host is running Lighttpd and is prone to remote code execution vulnerability. **Solution** Upgrade to Lighttpd 1.4.36 or later, For updates refer to to http://www.lighttpd.net **Affected Nodes** 192.168.0.241, 192.168.0.242, 192.168.1.240
5	**Missing httpOnly Cookie Attribute** **Summary** The application is missing the 'httpOnly' cookie attribute **Solution** Set the 'httpOnly' attribute for any session cookies.

CVSS	Recommendation
	Affected Nodes 192.168.1.1, 192.168.5.1
5	**OpenSSH Denial of Service Vulnerability** **Summary** OpenSSH is prone to a remote denial-of-service vulnerability. **Solution** Updates are available. **Affected Nodes** 192.168.0.3, 192.168.1.203, 192.168.1.204, 192.168.1.205
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** 192.168.0.3, 192.168.1.24, 192.168.1.201, 192.168.1.202, 192.168.1.203, 192.168.1.204, 192.168.1.205, 192.168.6.82(MINTLINUX)
5	**PHP Fileinfo Component Denial of Service Vulnerability (Linux)** **Summary** This host is installed with PHP and is prone to denial of service vulnerability. **Solution** Upgrade to PHP version 5.6.0 For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
5	**PHP Multiple Denial of Service Vulnerabilities (Linux)** **Summary** This host is installed with PHP and is prone to multiple denial of service vulnerabilities. **Solution** Upgrade to PHP version 5.6.12 or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
5	**Chargen** **Summary** The remote host is running a 'chargen' service. Description : When contacted, chargen responds with some random characters (something like all the characters in the alphabet in a row). When contacted via UDP, it will respond with a single UDP packet. When contacted via TCP, it will continue spewing characters until the client closes the connection. The purpose

CVSS	Recommendation
	of this service was to mostly to test the TCP/IP protocol by itself, to make sure that all the packets were arriving at their destination unaltered. It is unused these days, so it is suggested you disable it, as an attacker may use it to set up an attack against this host, or against a third party host using this host as a relay. An easy attack is 'ping-pong' in which an attacker spoofs a packet between two machines running chargen. This will cause them to spew characters at each other, slowing the machines down and saturating the redi. **Solution** - Under Unix systems, comment out the 'chargen' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry codes to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpChargen HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpChargen Then launch cmd.exe and type : net stop simptcp net start simptcp To restart the service. **Affected Nodes** 192.168.7.68(REMOTE)
5	**Quote of the day** **Summary** The quote service (qotd) is running on this host. Description : A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote. Another quote of the day service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 17. When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored). An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the redi. **Solution** - Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry codes to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd Then launch cmd.exe and type : net stop simptcp net start simptcp To restart the service. **Affected Nodes** 192.168.7.68(REMOTE)
5	**Dropbear SSH Server Multiple Security Vulnerabilities** **Summary** This host is installed with Dropbear SSH Server and is prone to multiple vulnerabilities. **Solution** Updates are available. **Affected Nodes** 192.168.1.240
5	**Microsoft IIS Default Welcome Page Information Disclosure Vulnerability** **Summary** The host is running Microsoft IIS Webserver and is prone to information disclosure

CVSS	Recommendation
	vulnerability. **Solution** Disable the default pages within the server configuration. **Affected Nodes** 192.168.1.21, 192.168.1.69, 192.168.1.81, 192.168.6.142(QB01)
5	**Microsoft Windows SMTP Server MX Record Denial of Service Vulnerability** **Summary** The Microsoft Windows Simple Mail Transfer Protocol (SMTP) Server is prone to a denial-of-service vulnerability and to to an information-disclosure vulnerability. Successful exploits of the denial-of-service vulnerability will cause the affected SMTP server to stop responding, denying service to legitimate accts. Attackers can exploit the information-disclosure issue to gain access to sensitive information. Any information obtained may lead to further attacks. **Solution** Microsoft released fixes to address this issue. Please see the references for more information. **Affected Nodes** 192.168.7.68(REMOTE)
5	**PHP open_basedir Security Bypass Vulnerability** **Summary** This host is installed with PHP and is prone to security bypass 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** 192.168.1.50(myco-bdr)
5	**PHP CDF File Parsing Denial of Service Vulnerabilities - 01 - Jun14** **Summary** This host is installed with PHP and is prone to denial of service vulnerabilities. **Solution** Upgrade to PHP version 5.4.29 or 5.5.13 or later. For updates refer to http://php.net **Affected Nodes** 192.168.1.50(myco-bdr)
4.9	**Samba Denial of Service Vulnerability** **Summary** This host is running Samba and is prone to denial of service vulnerability. **Solution** Upgrade to Samba 4.1.23 or 4.2.9 or 4.3.6 or 4.4.0rc4 later. For updates refer to https://www.samba.org/

CVSS	Recommendation
	Affected Nodes 192.168.6.82(MINTLINUX)
4.6	**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 acct codes. 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** 192.168.1.24, 192.168.1.201, 192.168.1.202, 192.168.6.82(MINTLINUX)
4.3	**OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (FREAK)** **Summary** This host is installed with OpenSSL and is prone to man in the middle attack. **Solution** Remove support for EXPORT_RSA cipher suites from the service. Update to version 0.9.8zd or 1.0.0p or 1.0.1k or later For updates refer to https://www.openssl.org **Affected Nodes** 192.168.1.201, 192.168.1.202, 192.168.1.203
4.3	**OpenSSL TLS DHE_EXPORT LogJam Man in the Middle Security Bypass Vulnerability** **Summary** This host is installed with OpenSSL and is prone to man in the middle attack. **Solution** Remove support for DHE_EXPORT cipher suites from the service or Update to version 1.0.2b or 1.0.1n or later, For updates refer to https://www.openssl.org **Affected Nodes** 192.168.1.201, 192.168.1.202
4.3	**PHP display_errors Cross Site Scripting Vulnerability** **Summary** This host is installed with PHP and is prone to cross site scripting vulnerability. **Solution** Upgrade to latest version of PHP, http://www.php.net/downloads.php **Affected Nodes** 192.168.1.50(myco-bdr)

CVSS	Recommendation
4.3	**PHP Cross-Site Scripting Vulnerability - Aug16 (Linux)** **Summary** This host is installed with PHP and is prone to cross-site scripting (XSS) vulnerability. **Solution** Upgrade to PHP version 5.4.38, or 5.5.22, or 5.6.6, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)
4.3	**PHP SOAP Parser Multiple Information Disclosure Vulnerabilities** **Summary** This host is installed with PHP and is prone to multiple information disclosure vulnerabilities. **Solution** Upgrade to PHP 5.3.22 or 5.4.12 or later, http://www.php.net/downloads.php **Affected Nodes** 192.168.1.50(myco-bdr)
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** 192.168.0.241, 192.168.1.1, 192.168.1.5(VPNGW), 192.168.1.15(UTIL12), 192.168.1.21, 192.168.1.69, 192.168.1.81, 192.168.1.203, 192.168.1.205, 192.168.1.240, 192.168.5.1, 192.168.6.5, 192.168.6.49, 192.168.6.142(QB01), 192.168.6.154, 192.168.6.159(VPNGW)
4.3	**POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability** **Summary** This host is prone to an information disclosure vulnerability. **Solution** Disable SSL v3.0 **Affected Nodes** 192.168.1.1, 192.168.1.5(VPNGW), 192.168.1.15(UTIL12), 192.168.1.21, 192.168.1.69, 192.168.1.81, 192.168.1.203, 192.168.1.205, 192.168.1.240, 192.168.5.1, 192.168.6.5, 192.168.6.49, 192.168.6.142(QB01), 192.168.6.154, 192.168.6.159(VPNGW)
4.3	**PHP LibGD Denial of Service Vulnerability** **Summary** This host is installed with PHP and is prone to denial of service vulnerability. **Solution**

CVSS	Recommendation
	Upgrade to PHP version 5.4.32 or 5.5.16 or 5.6.0 or later. For updates refer to http://php.net **Affected Nodes** 192.168.1.50(myco-bdr)
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** 192.168.0.3, 192.168.0.11, 192.168.1.1, 192.168.1.24, 192.168.1.201, 192.168.1.202, 192.168.1.203, 192.168.1.204, 192.168.1.205, 192.168.1.240, 192.168.5.1, 192.168.6.49, 192.168.6.82(MINTLINUX), 192.168.6.153
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** 192.168.0.3, 192.168.1.24, 192.168.1.203, 192.168.1.204, 192.168.1.205, 192.168.6.82(MINTLINUX)

Low Risk

CVSS	Recommendation
4	**SSL Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability** **Summary** The 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 https://weakdh.org/sysadmin.html) **Affected Nodes** 192.168.1.1, 192.168.1.203, 192.168.1.205, 192.168.5.1, 192.168.6.49
4	**SSL Certificate Signed Using A Weak Signature Algorithm** **Summary** The remote service is using a SSL certificate chain that has been signed using a cryptographically weak hashing algorithm. **Solution**

CVSS	Recommendation
	Affected Nodes 192.168.0.11, 192.168.1.1, 192.168.1.3(DC03), 192.168.1.4, 192.168.1.5(VPNGW), 192.168.1.15(UTIL12), 192.168.1.16(sourcesvr), 192.168.1.21, 192.168.1.23, 192.168.1.31(HVFS), 192.168.1.32(HVFS), 192.168.1.33(HVFS), 192.168.1.34(HVFS), 192.168.1.41(FILE2012-1), 192.168.1.63(PITWDS12), 192.168.1.64(PITWDS12), 192.168.1.65(STORAGE12), 192.168.1.66(STORAGE12), 192.168.1.67(STORAGE12), 192.168.1.69, 192.168.1.81, 192.168.1.100(HV00), 192.168.1.104(HV04), 192.168.1.121(HV02), 192.168.1.122(HV02), 192.168.1.123(HV02), 192.168.1.203, 192.168.1.205, 192.168.1.240, 192.168.5.1, 192.168.6.5, 192.168.6.10(WIN7-TEMP-1), 192.168.6.11, 192.168.6.14(Psolidad-WIN764), 192.168.6.16(svr1-65LI), 192.168.6.21(svr1-99ZO), 192.168.6.30(Mwest-WIN864), 192.168.6.44(b2b-GW), 192.168.6.45(DESKTOP-UAE29E6), 192.168.6.47, 192.168.6.48(svr1-99ZP), 192.168.6.49, 192.168.6.57(svr1-99ZW), 192.168.6.67(sourcesvrBUILD), 192.168.6.70(WIN-888AUK4TQ2S), 192.168.6.73(WIN-D1LTOO0FR17), 192.168.6.80(darkhorse), 192.168.6.86(WIN-UH2DKI2HMN4), 192.168.6.87(svr1-91OD), 192.168.6.88(WIN-1OOISUH62LO), 192.168.6.92, 192.168.6.96, 192.168.6.100(HV04), 192.168.6.105(HV04), 192.168.6.107(svr1-99ZB), 192.168.6.108(HV04), 192.168.6.112(REX), 192.168.6.120(PKWIN8-VM), 192.168.6.123(HV01), 192.168.6.124(HV01), 192.168.6.130(porchanko-HOME), 192.168.6.132(SARLACC), 192.168.6.142(QB01), 192.168.6.150(workstation-TEST1), 192.168.6.151(HV01), 192.168.6.159(VPNGW), 192.168.7.44(JIM-WIN8), 192.168.7.95(Mmichaels-HP), 192.168.7.99(PS01), 192.168.7.123(ISTCORP-PC)
4	**Samba Overwrite ACLs Vulnerability** **Summary** This host is running Samba and is prone to overwrite ACLs vulnerability. **Solution** Upgrade to Samba version 4.1.23 or 4.2.9 or 4.3.6 or 4.4.0rc4 or later. For updates refer to https://www.samba.org **Affected Nodes** 192.168.1.50(myco-bdr), 192.168.6.82(MINTLINUX)
4	**ISC BIND AXFR Response Denial of Service Vulnerability** **Summary** ISC BIND is prone to a denial of service vulnerability. **Solution** No solution or patch is available as of 15th September, 2016. Information regarding this issue will be updated once the solution details are available. **Affected Nodes** 192.168.3.2
3.5	**openssh-server Forced dbre Handling Information Disclosure Vulnerability** **Summary** The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_codes dbre options, which allows remote authenticated accts to obtain potentially sensitive information by reading these messages, as demonstrated by the shared acct account required by Gitolite. NOTE: this can cross privilege boundaries because a acct account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an authorized_codes file in its own home

CVSS	Recommendation
	directory. **Solution** Updates are available. Please see the references for more information. **Affected Nodes** 192.168.0.3, 192.168.1.203, 192.168.1.204, 192.168.1.205
3.5	**OpenSSH ssh_gssapi_parse_ename() Function Denial of Service Vulnerability** **Summary** OpenSSH is prone to a remote denial-of-service vulnerability. **Solution** Updates are available. Please see the references for details. **Affected Nodes** 192.168.0.3, 192.168.1.203, 192.168.1.204, 192.168.1.205
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** 192.168.0.2, 192.168.0.11, 192.168.0.241, 192.168.0.242, 192.168.1.3(DC03), 192.168.1.4, 192.168.1.5(VPNGW), 192.168.1.15(UTIL12), 192.168.1.16(sourcesvr), 192.168.1.21, 192.168.1.23, 192.168.1.24, 192.168.1.31(HVFS), 192.168.1.32(HVFS), 192.168.1.33(HVFS), 192.168.1.34(HVFS), 192.168.1.41(FILE2012-1), 192.168.1.50(myco-bdr), 192.168.1.52, 192.168.1.63(PITWDS12), 192.168.1.64(PITWDS12), 192.168.1.65(STORAGE12), 192.168.1.66(STORAGE12), 192.168.1.67(STORAGE12), 192.168.1.69, 192.168.1.81, 192.168.1.100(HV00), 192.168.1.104(HV04), 192.168.1.121(HV02), 192.168.1.122(HV02), 192.168.1.123(HV02), 192.168.1.201, 192.168.1.202, 192.168.1.203, 192.168.1.204, 192.168.1.205, 192.168.1.240, 192.168.1.254(monitor-GW), 192.168.3.2, 192.168.6.5, 192.168.6.7, 192.168.6.9(HPDT-8CC5260NXY), 192.168.6.10(WIN7-TEMP-1), 192.168.6.12(Psolidad-PC), 192.168.6.14(Psolidad-WIN764), 192.168.6.16(svr1-65LI), 192.168.6.21(svr1-99ZO), 192.168.6.22, 192.168.6.26(HPLT-5CD4411D8Z), 192.168.6.30(Mwest-WIN864), 192.168.6.37(betty-INSPIRON), 192.168.6.44(b2b-GW), 192.168.6.45(DESKTOP-UAE29E6), 192.168.6.47, 192.168.6.48(svr1-99ZP), 192.168.6.49, 192.168.6.52(WILLARD), 192.168.6.56(CONFERENCE-ROOM), 192.168.6.57(svr1-99ZW), 192.168.6.63(buildbox), 192.168.6.67(sourcesvrBUILD), 192.168.6.68(FRONTDOOR), 192.168.6.70(WIN-888AUK4TQ2S), 192.168.6.73(WIN-D1LTOO0FR17), 192.168.6.79(Mcarrier-ASUS), 192.168.6.80(darkhorse), 192.168.6.81(Lalexander-PC), 192.168.6.82(MINTLINUX), 192.168.6.86(WIN-UH2DKI2HMN4), 192.168.6.87(svr1-91OD),

CVSS	Recommendation
	192.168.6.88(WIN-1OOISUH62LO), 192.168.6.92, 192.168.6.96, 192.168.6.100(HV04), 192.168.6.105(HV04), 192.168.6.107(svr1-99ZB), 192.168.6.108(HV04), 192.168.6.112(REX), 192.168.6.120(PKWIN8-VM), 192.168.6.123(HV01), 192.168.6.124(HV01), 192.168.6.125(WAMPA), 192.168.6.126(Tneusome-HP), 192.168.6.128, 192.168.6.130(porchanko-HOME), 192.168.6.132(SARLACC), 192.168.6.133(PANOPTICON), 192.168.6.142(QB01), 192.168.6.150(workstation-TEST1), 192.168.6.151(HV01), 192.168.6.154, 192.168.6.159(VPNGW), 192.168.6.161(ROWBOT), 192.168.6.165(IRIDIUM), 192.168.6.195(tarsis), 192.168.7.44(JIM-WIN8), 192.168.7.95(Mmichaels-HP), 192.168.7.99(PS01), 192.168.7.123(ISTCORP-PC)
2.6	**Relative IP Identification number change** **Summary** The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host. **Solution** Contact your vendor for a patch **Affected Nodes** 192.168.0.2, 192.168.1.1, 192.168.1.31(HVFS), 192.168.1.52, 192.168.5.1, 192.168.6.153
2.6	**PHP Information Disclosure Vulnerability - 01 - Sep14** **Summary** This host is installed with PHP and is prone to information disclosure vulnerability. **Solution** Upgrade to PHP version 5.3.29 or 5.4.30 or 5.5.14 or later **Affected Nodes** 192.168.1.50(myco-bdr)
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** 192.168.0.3, 192.168.0.11, 192.168.1.24, 192.168.1.203, 192.168.1.204, 192.168.1.205, 192.168.1.240, 192.168.6.49, 192.168.6.82(MINTLINUX), 192.168.6.153
2.6	**OpenSSH CBC Mode Information Disclosure Vulnerability** **Summary** The host is installed with OpenSSH and is prone to information disclosure vulnerability. **Solution** Upgrade to higher version http://www.openssh.com/portable.html **Affected Nodes** 192.168.0.3, 192.168.1.205

CVSS	Recommendation
2.1	**OpenSSH ssh-codesign.c Local Information Disclosure Vulnerability** **Summary** OpenSSH is prone to a local information-disclosure vulnerability. **Solution** Updates are available. **Affected Nodes** 192.168.0.3, 192.168.1.203, 192.168.1.204, 192.168.1.205