YourIT!
Your Logo Goes Here

Security Assessment

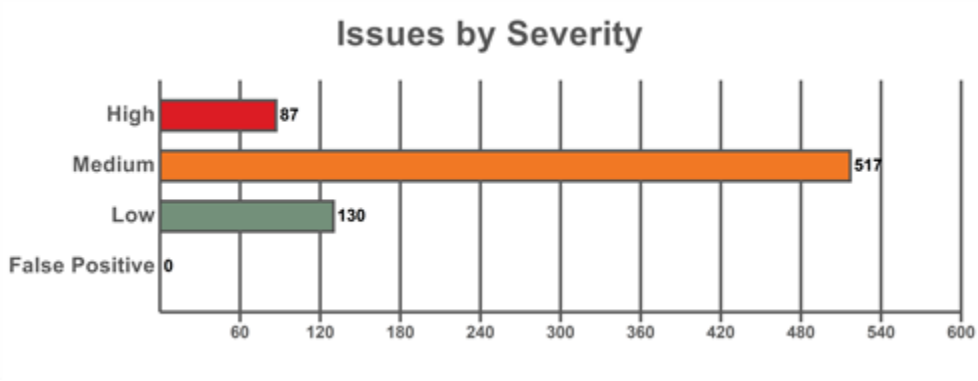
Internal Vulnerability Scan Detail by Issue Report

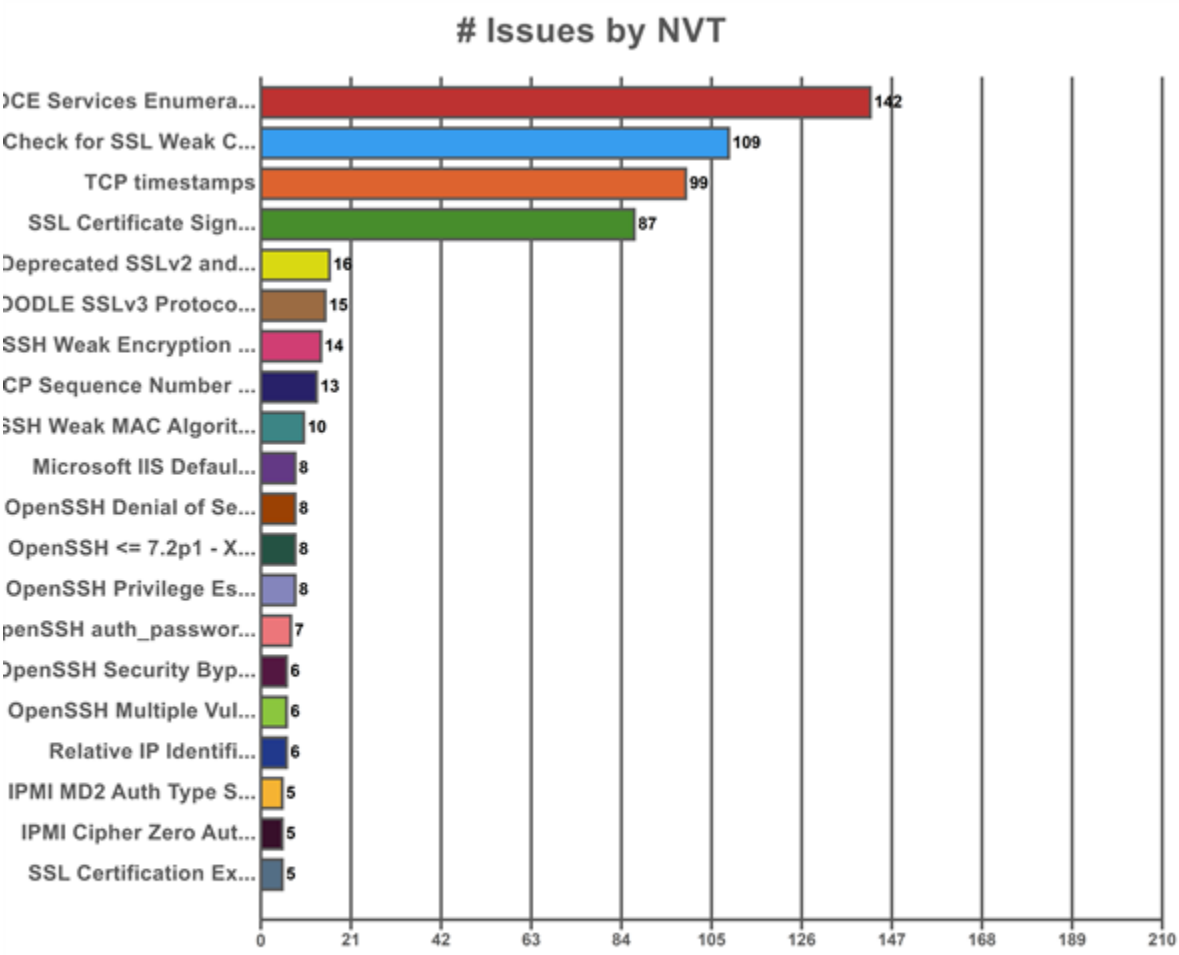
Prepared for:
Your Customer / Prospect
Prepared by:
Your Company Name

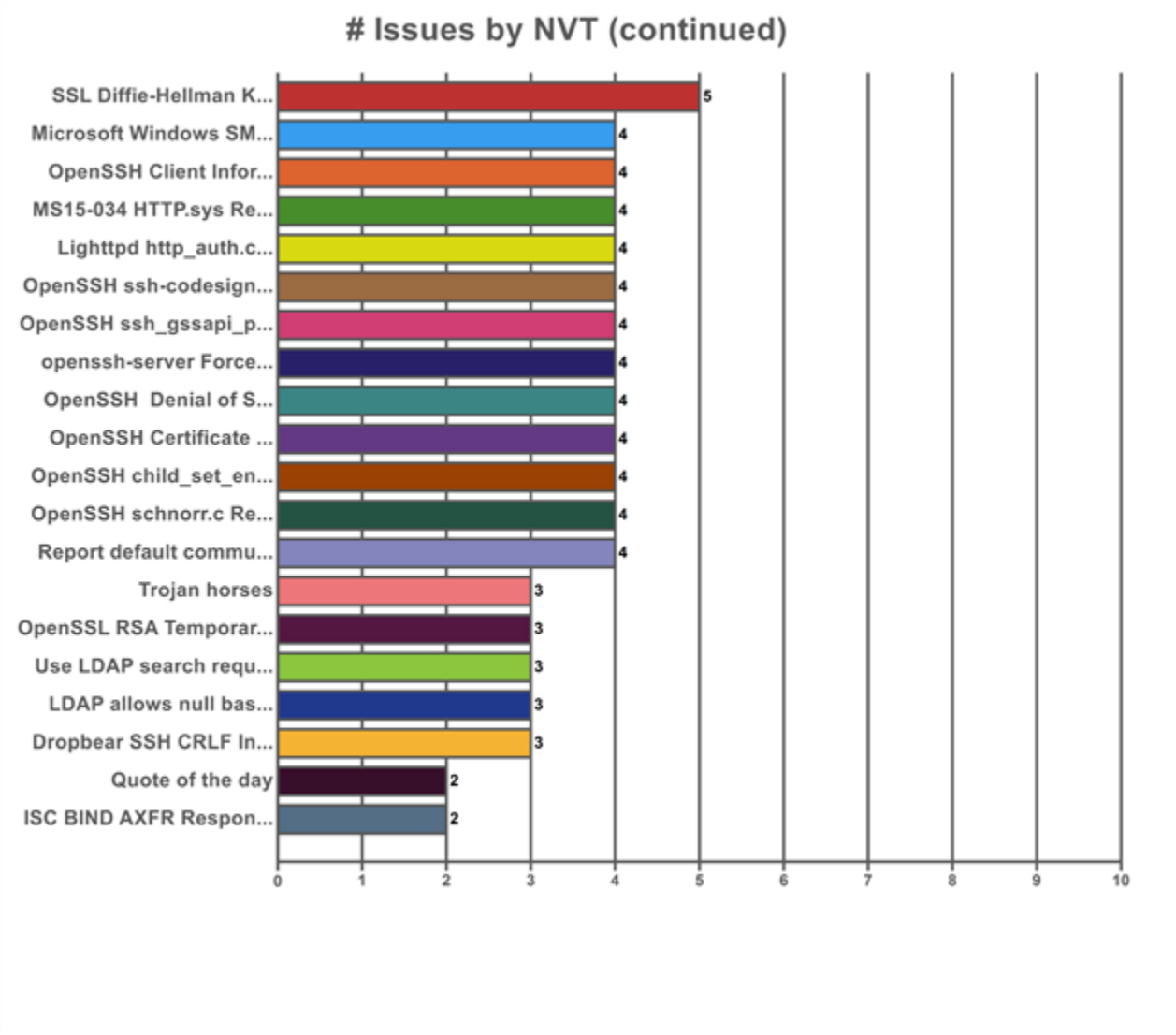
Table of Contents

1 - Summary

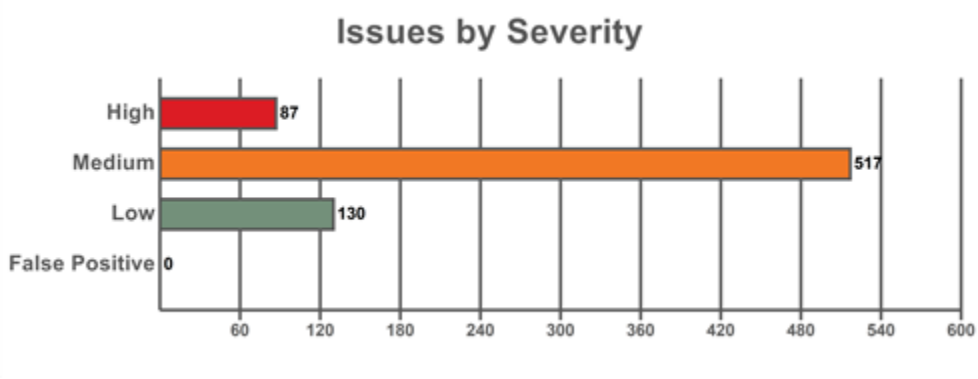
This report gives details on hosts that were tested and issues that were found group by individual issues.






Issues by NVT (continued)
SSL Diffie-Hellman K... 5
Microsoft Windows SM... 4
OpenSSH Client Infor... 4
MS15-034 HTTP.sys Re... 4
Lighttpd http_auth.c... 4
OpenSSH ssh-codesign... 4
OpenSSH ssh_gssapi_p... 4
openssh-server Force... 4
OpenSSH Denial of S... 4
OpenSSH Certificate ... 4
OpenSSH child_set_en... 4
OpenSSH schnorr.c Re... 4
Report default commu... 4
Trojan horses 3
OpenSSL RSA Temporar... 3
Use LDAP search requ... 3
LDAP allows null bas... 3
Dropbear SSH CRLF In... 3
Quote of the day 2
ISC BIND AXFR Respon... 2
0 1 2 3 4 5 6 7 8 9 10

2 - Scan Details



2.1 - PHP phar_fix_filepath Function Stack Buffer Overflow Vulnerability - Mar16 (Linux)

H **High**: (CVSS: 10)
OID: 1.3.6.1.4.1.25623.1.0.807507 — 80/tcp (http)

Summary
This host is installed with PHP and is prone to stack buffer overflow vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.4.43

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the PHP process. Failed exploit attempts will likely crash the webserver. Impact Level: Application

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

Vulnerability Insight
Multiple flaws are due to - Inadequate boundary checks on acct-supplied input by 'phar_fix_filepath' function in 'ext/phar/phar.c' script. - Improper validation of file pointer in the 'phar_convert_to_other' function in 'ext/phar/phar_object.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16... (OID: 1.3.6.1.4.1.25623.1.0.807507) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php, https://bugs.php.net/bug.php?id=69923

2.2 - Trojan horses

H **High**: (CVSS: 10)
OID: 1.3.6.1.4.1.25623.1.0.11157 — 2002/tcp

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.

Affected Nodes
192.168.6.14(Psolidad-WIN764), 192.168.6.30(Mwest-WIN864), 192.168.7.68(REMOTE)

Vulnerability Detection Result
An unknown service runs on this port. It is sometimes opened by this/these Trojan horse(s): Singu Slapper W32.Beagle Unless you know for sure what is behind it, you'd better check your system *** Anyway, don't panic, OpenVAS only found an open port. It may *** have been dynamically allocated to some service (RPC...) Solution: if a trojan horse is running, run a good antivirus scanner
Multiple results by host

Solution
if a trojan horse is running, run a good antivirus scanner

Vulnerability Detection Method
Details: Trojan horses (OID: 1.3.6.1.4.1.25623.1.0.11157) Version used: $Revision: 4034 $

2.3 - VMSA-2015-0007: VMware ESXi OpenSLP Remote Code Execution (remote check)

H **High**: (CVSS: 10)
OID: 1.3.6.1.4.1.25623.1.0.105394

Summary
VMware vCenter and ESXi updates address critical security issues.

Affected Nodes
192.168.6.154

Vulnerability Detection Result
ESXi Version: 5.5.0 Detected Build: 2403361 Fixed Build: 3029944

Solution
Apply the missing patch(es).

Vulnerability Insight
VMware ESXi OpenSLP Remote Code Execution VMware ESXi contains a double free flaw in OpenSLP's SLPDProcessMessage() function. Exploitation of this issue may allow an unauthenticated attacker to execute code remotely on the ESXi host. VMware vCenter Server JMX RMI Remote Code Execution VMware vCenter Server contains a remotely accessible JMX RMI service that is not securely configured. An unauthenticated remote attacker that is able to connect to the service may be able use it to execute arbitrary code on the vCenter server. VMware vCenter Server vpxd denial-of-service vulnerability VMware vCenter Server does not properly sanitize long heartbeat messages. Exploitation of this issue may allow an unauthenticated attacker to create a denial-of-service condition in the vpxd service.

Vulnerability Detection Method
Check the build number Details: VMSA-2015-0007: VMware ESXi OpenSLP Remote Code Execution (remote check) (OID: 1.3.6.1.4.1.25623.1.0.105394) Version used: $Revision: 2748 $

References
http://www.vmware.com/security/advisories/VMSA-2015-0007.html

2.4 - PHP End Of Life Detection (Linux)

H **High**: (CVSS: 10)
OID: 1.3.6.1.4.1.25623.1.0.105889 80/tcp (http)

Summary
The PHP version on the remote host has reached the end of life and should not be used anymore.

Affected Nodes

192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.6/7.0

Impact
An end of life version of PHP is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution
Update the PHP version on the remote host to a still supported version.

Vulnerability Insight
Each release branch of PHP is fully supported for two years from its initial stable release. During this period, bugs and security issues that have been reported are fixed and are released in regular point releases. After this two year period of active support, each branch is then supported for an additional year for critical security issues only. Releases during this period are made on an as-needed basis: there may be multiple point releases, or none, depending on the number of reports. Once the three years of support are completed, the branch reaches its end of life and is no longer supported.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is unsupported. Details: PHP End Of Life Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.105889) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
https://secure.php.net/supported-versions.php

2.5 - NFS export

H **High**: (CVSS: 10)
OID: 1.3.6.1.4.1.25623.1.0.102014 — 2049/udp (nfs)

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

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Here is the export list of 192.168.1.50 : /home/appsvr30Dev 0.0.0.0/0.0.0.0 Please check the permissions of this exports.

Vulnerability Detection Method
Details: NFS export (OID: 1.3.6.1.4.1.25623.1.0.102014) Version used: $Revision: 3604 $

2.6 - IPMI Cipher Zero Authentication Bypass Vulnerability

H **High**: (CVSS: 10)
OID: 1.3.6.1.4.1.25623.1.0.103840 — 623/tcp

Summary
Intelligent Platform Management Interface is prone to an authentication- bypass vulnerability.

Affected Nodes
192.168.1.201, 192.168.1.202, 192.168.1.203, 192.168.1.204, 192.168.1.205

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Attackers can exploit this issue to gain administrative access to the device and disclose sensitive information.

Solution
Ask the Vendor for an update.

Vulnerability Insight
The remote IPMI service accepted a session open request for cipher zero.

Vulnerability Detection Method
Send a request with a zero cipher and check if this request was accepted. Details: IPMI Cipher Zero Authentication Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103840) Version used: $Revision: 2939 $

References
http://fish2.com/ipmi/cipherzero.html

2.7 - PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Linux)

H **High**: (CVSS: 10) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.808607

Summary
This host is installed with PHP and is prone to denial of service and unspecified Vulnerabilities

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.5.32

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact. Impact Level: Application

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

Vulnerability Insight
The flaw is due an improper handling of zero-length uncompressed data in 'ext/phar/phar_object.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808607) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-7.php, http://www.openwall.com/lists/oss-security/2016/04/28/2

2.8 - PHP type confusion Denial of Service Vulnerability (Linux)

H **High**: (CVSS: 10) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.808673

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.6.7

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service. Impact Level: Application

Solution
Upgrade to PHP version 5.6.7 or later. For updates refer to http://www.php.net

Vulnerability Insight
The flaw is due to 'type confusion' issues in 'ext/soap/php_encoding.c', 'ext/soap/php_http.c', and 'ext/soap/soap.c' scripts.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP 'type confusion' Denial of Service Vulnerability (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808673) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php

2.9 - ProFTPD `mod_copy` Unauthenticated Copying Of Files Via SITE CPFR/CPTO

H **High**: (CVSS: 10)
OID: 1.3.6.1.4.1.25623.1.0.105254 — 21/tcp (ftp)

Summary
ProFTPD is prone to an unauthenticated copying of files vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Under some circumstances this could result in remote code execution

Solution
Ask the vendor for an update

Vulnerability Detection Method
Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO Details: ProFTPD `mod_copy` Unauthenticated Copying Of Files Via SITE CPFR/CPTO (OID: 1.3.6.1.4.1.25623.1.0.105254) Version used: $Revision: 2676 $

References
http://bugs.proftpd.org/show_bug.cgi?id=4169

2.10 - Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

H **High**: (CVSS: 10)
OID: 1.3.6.1.4.1.25623.1.0.902269 — 445/tcp (microsoft-ds)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS10-012.

Affected Nodes
192.168.7.68(REMOTE)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service or bypass the authentication mechanism via brute force technique. Impact Level: System/Application

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

Vulnerability Insight
- An input validation error exists while processing SMB requests and can be exploited to cause a buffer overflow via a specially crafted SMB packet. - An error exists in the SMB implementation while parsing SMB packets during the Negotiate phase causing memory corruption via a specially crafted SMB packet. - NULL pointer dereference error exists in SMB while verifying the 'share' and 'servername' fields in SMB packets causing denial of service. - A lack of cryptographic entropy when the SMB server generates challenges during SMB NTLM authentication and can be exploited to bypass the authentication mechanism.

Vulnerability Detection Method
Details: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468) (OID: 1.3.6.1.4.1.25623.1.0.902269) Version used: $Revision: 4161 $

References
http://secunia.com/advisories/38510/, http://support.microsoft.com/kb/971468, http://www.vupen.com/english/advisories/2010/0345, http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx

2.11 - MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check)

H **High**: (CVSS: 10) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.105257

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-034.

Affected Nodes
192.168.1.5(VPNGW), 192.168.1.15(UTIL12), 192.168.6.159(VPNGW)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current acct and to perform actions in the security context of the current acct.

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

Vulnerability Insight
Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.

Vulnerability Detection Method
Send a special crafted HTTP GET request and check the response Details: MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check) (OID: 1.3.6.1.4.1.25623.1.0.105257) Version used: $Revision: 2646 $

References
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1635, https://support.microsoft.com/kb/3042553, https://technet.microsoft.com/library/security/MS15-034, http://pastebin.com/ypURDPc4

2.12 - Samba TALLOC_FREE() Function Remote Code Execution Vulnerability

H **High**: (CVSS: 10)
OID: 1.3.6.1.4.1.25623.1.0.105231

Summary
Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability

Affected Nodes
192.168.1.50(myco-bdr), 192.168.6.82(MINTLINUX)

Vulnerability Detection Result
Installed version: 3.6.3 Fixed version: 3.6.25 or 4.0.25 or 4.1.17, 4.2.0rc5, or later
Multiple results by host

Impact
An attacker can exploit this issue to execute arbitrary code with root privileges. Failed exploit attempts will cause a denial-of-service condition

Solution
Updates are available. Please see the references or vendor advisory for more information.

Vulnerability Insight
The Netlogon server implementation in smbd performs a free operation on an uninitialized stack pointer, which allows remote attackers to execute arbitrary code via crafted Netlogon packets that use the ServerPasswordSet RPC API, as demonstrated by packets reaching the _netr_ServerPasswordSet function in rpc_server/netlogon/srv_netlog_nt.c.

Vulnerability Detection Method
Check the version Details: Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.105231) Version used: $Revision: 3901 $

References
http://www.securityfocus.com/bid/72711, http://www.samba.org

2.13 - Discard port open

H **High**: (CVSS: 10) 9/tcp (discard)
OID: 1.3.6.1.4.1.25623.1.0.11367

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 advised that you disable it.

Affected Nodes
192.168.7.68(REMOTE)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

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.

Vulnerability Detection Method
Details: Discard port open (OID: 1.3.6.1.4.1.25623.1.0.11367) Version used: $Revision: 3780 $

2.14 - Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387)

H **High**: (CVSS: 9.3) 3389/tcp
OID: 1.3.6.1.4.1.25623.1.0.902818

Summary
This host is missing a critical security update according to Microsoft Bulletin MS12-020.

Affected Nodes
192.168.7.68(REMOTE)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow remote attackers to execute arbitrary code as the logged-on acct or cause a denial of service condition. Impact Level: System/Application

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

Vulnerability Insight
The flaws are due to the way Remote Desktop Protocol accesses an object in memory that has been improperly initialized or has been deleted and the way RDP service processes the packets.

Vulnerability Detection Method
Details: Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (267... (OID: 1.3.6.1.4.1.25623.1.0.902818) Version used: $Revision: 4234 $

References
http://blog.binaryninjas.org/?p=58, http://secunia.com/advisories/48395, http://support.microsoft.com/kb/2671387, http://www.securitytracker.com/id/1026790, http://technet.microsoft.com/en-us/security/bulletin/ms12-020

2.15 - SSH Brute Force Logins with default Credentials

H **High**: (CVSS: 9)
OID: 1.3.6.1.4.1.25623.1.0.103239 — 22/tcp (ssh)

Summary
A number of known default credentials is tried for log in via SSH protocol.

Affected Nodes
192.168.1.1, 192.168.5.1

Vulnerability Detection Result
It was possible to login with the following credentials <acct>:<Password> admin:password

Solution
Change the password as soon as possible.

Vulnerability Detection Method
Details: SSH Brute Force Logins with default Credentials (OID: 1.3.6.1.4.1.25623.1.0.103239) Version used: $Revision: 3920 $

2.16 - Microsoft SQL Server Multiple Vulnerabilities (3065718) - Remote

H **High**: (CVSS: 8.5)
OID: 1.3.6.1.4.1.25623.1.0.805815

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-058.

Affected Nodes
192.168.1.16(sourcesvr)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to elevate the privileges or execute arbitrary code remotely. Impact Level: System/Application

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

Vulnerability Insight
Flaws exist due to, - An improperly casts pointers to an incorrect class. - An incorrectly handling itable function calls to uninitialized memory.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: Microsoft SQL Server Multiple Vulnerabilities (3065718) - Remote (OID: 1.3.6.1.4.1.25623.1.0.805815) Version used: $Revision: 2646 $

Product Detection Result
Product: cpe:/a:microsoft:sql_server:11.0.3128.0 Method: Microsoft SQL TCP/IP listener is running (OID: 1.3.6.1.4.1.25623.1.0.10144)

References
https://support.microsoft.com/en-us/kb/3065718, https://technet.microsoft.com/library/security/MS15-058

2.17 - OpenSSH Multiple Vulnerabilities

H **High**: (CVSS: 8.5) 22/tcp (ssh)
OID: 1.3.6.1.4.1.25623.1.0.806052

Summary
This host is running OpenSSH and is prone to multiple vulnerabilities.

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)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: 7.0
Multiple results by host

Impact
Successful exploitation will allow an attacker to gain privileges, to conduct impersonation attacks, to conduct brute-force attacks or cause a denial of service. Impact Level: Application

Solution
Upgrade to OpenSSH 7.0 or later. For updates refer to http://www.openssh.com

Vulnerability Insight
Multiple flaws are due to: - Use-after-free vulnerability in the 'mm_answer_pam_free_ctx' function in monitor.c in sshd. - Vulnerability in 'kbdint_next_device' function in auth2-chall.c in sshd. - vulnerability in the handler for the MONITOR_REQ_PAM_FREE_CTX request.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: OpenSSH Multiple Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.806052) Version used: $Revision: 2676 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.3 Method: SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

References
http://seclists.org/fulldisclosure/2015/Aug/54, http://openwall.com/lists/oss-security/2015/07/23/4

2.18 - OpenSSH auth_password Denial of Service Vulnerability (Linux)

H **High**: (CVSS: 7.8) 22/tcp (ssh)
OID: 1.3.6.1.4.1.25623.1.0.809154

Summary
This host is installed with openssh and is prone to denial of service vulnerability.

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)

Vulnerability Detection Result
Installed version: 6.6.1p1 Fixed version: 7.3
Multiple results by host

Impact
Successfully exploiting this issue allows remote attackers to cause a denial of service (crypt CPU consumption).
Impact Level: Application

Solution
Upgrade to OpenSSH version 7.3 or later. For updates refer to http://www.openssh.com

Vulnerability Insight
The flaw exists due to the auth_password function in 'auth-passwd.c' script does not limit password lengths for password authentication.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: OpenSSH 'auth_password' Denial of Service Vulnerability (Linux) (OID: 1.3.6.1.4.1.25623.1.0.809154) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:6.6.1p1 Method: SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

References
http://www.openssh.com/txt/release-7.3, http://openwall.com/lists/oss-security/2016/08/01/2

2.19 - PHP Arbitrary Code Execution Vulnerability - Aug16 (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.808671

Summary
This host is installed with PHP and is prone to arbitrary code execution vulnerability

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.5.27

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation. Impact Level: Application

Solution
Upgrade to PHP version 5.5.27, or 5.6.11, or later. For updates refer to http://www.php.net

Vulnerability Insight
The flaw is due to Use-after-free vulnerability in the 'spl_ptr_heap_insert' function in 'ext/spl/spl_heap.c'.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Arbitrary Code Execution Vulnerability - Aug16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808671) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php

2.20 - PHP Multiple Vulnerabilities - 02 - Aug16 (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.808790

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.5.37

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (use-after-free and application crash) or possibly execute arbitrary code or possibly have unspecified other impact via a large integer argument. Impact Level: Application

Solution
Upgrade to PHP version 5.5.37, or 5.6.23, or later. For updates refer to http://www.php.net

Vulnerability Insight
Multiple flaws are due to, - The 'spl_array.c' in the SPL extension improperly interacts with the unserialize implementation and garbage collection. - The integer overflow in the 'SplFileObject::fread' function in 'spl_directory.c' in the SPL extension.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Vulnerabilities - 02 - Aug16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808790) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php

2.21 - PHP Multiple Vulnerabilities - 01 - Aug16 (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.808788

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.5.37

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code. Impact Level: Application

Solution
Upgrade to PHP version 5.5.37, or 5.6.23, or 7.0.8, or later. For updates refer to http://www.php.net

Vulnerability Insight
Multiple flaws are due to, - The 'php_zip.c' script in the zip extension improperly interacts with the unserialize implementation and garbage collection. - The php_wddx_process_data function in 'wddx.c' script in the WDDX extension mishandled data in a wddx_deserialize call. - The multiple integer overflows in 'mcrypt.c' script in the mcrypt extension. - The double free vulnerability in the '_php_mb_regex_ereg_replace_exec' function in 'php_mbregex.c' script in the mbstring extension. - An integer overflow in the '_gd2GetHeader' function in 'gd_gd2.c' script in the GD Graphics Library. - An integer overflow in the 'gdImageCreate' function in 'gd.c' script in the GD Graphics Library.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Vulnerabilities - 01 - Aug16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808788) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php, http://www.php.net/ChangeLog-7.php

2.22 - PHP Multiple Vulnerabilities - 05 - Aug16 (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.808675

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.4.42

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, to read or write to arbitrary files, also execute arbitrary code via a long reply to a LIST dbre, leading to a heap-based buffer overflow. Impact Level: Application

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

Vulnerability Insight
The multiple flaws are due to, - Improper validation of token extraction for table names, in the php_pgsql_meta_data function in pgsql.c in the PostgreSQL extension. - Integer overflow in the ftp_genlist function in ext/ftp/ftp.c - PHP does not ensure that pathnames lack %00 sequences.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Vulnerabilities - 05 - Aug16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808675) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php

2.23 - PHP Multiple Vulnerabilities - 03 - Aug16 (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.808792

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.5.36

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service or possibly have unspecified other impact. Impact Level: Application

Solution
Upgrade to PHP version 5.5.36, or 5.6.22, or later. For updates refer to http://www.php.net

Vulnerability Insight
Multiple flaws are due to, - An integer overflow in the fread function in 'ext/standard/file.c' script. - An integer overflow in the php_html_entities function in 'ext/standard/html.c' script. - An Integer overflow in the php_escape_html_entities_ex function in 'ext/standard/html.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Vulnerabilities - 03 - Aug16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808792) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php

2.24 - PHP var_unserializer Denial of Service Vulnerability (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.809321

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.6.26

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service. Impact Level: Application

Solution
Upgrade to PHP version 5.6.26, or later. For updates refer to http://www.php.net

Vulnerability Insight
The flaw is due to improper handling of object-deserialization failures in 'ext/standard/var_unserializer.re' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP 'var_unserializer' Denial of Service Vulnerability (Linux) (OID: 1.3.6.1.4.1.25623.1.0.809321) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php

2.25 - PHP libgd Denial of Service Vulnerability (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.809338

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: Patch Available

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, or possibly have unspecified other impact. Impact Level: Application

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

Vulnerability Insight
The flaw exist due to an integer overflow in the gdImageWebpCtx function in gd_webp.c in the GD Graphics Library.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP 'libgd' Denial of Service Vulnerability (Linux) (OID: 1.3.6.1.4.1.25623.1.0.809338) Version used: $Revision: 4240 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-7.php, http://seclists.org/oss-sec/2016/q3/639

2.26 - PHP Multiple Vulnerabilities - 02 - Sep16 (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.809319

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.6.25

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, to obtain sensitive information from process memory, to inject arbitrary-type session data by leveraging control of a session name. Impact Level: Application

Solution
Upgrade to PHP version 5.6.25, or 7.0.10, or later. For updates refer to http://www.php.net

Vulnerability Insight
Multiple flaws are due to - An invalid wddxPacket XML document that is mishandled in a wddx_deserialize call in 'ext/wddx/wddx.c' script. - An error in 'php_wddx_pop_element' function in 'ext/wddx/wddx.c' script. - An error in 'php_wddx_process_data' function in 'ext/wddx/wddx.c' script. - Improper handling of the case of a thumbnail offset that exceeds the file size in 'exif_process_IFD_in_TIFF' function in 'ext/exif/exif.c' script. - Improper validation of gamma values in 'imagegammacorrect' function in 'ext/gd/gd.c' script. - Improper validation of number of colors in 'imagegammacorrect' function in 'ext/gd/gd.c' script. - The script 'ext/session/session.c' skips invalid session names in a way that triggers incorrect parsing. - Improper handling of certain objects in 'ext/standard/var_unserializer.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Vulnerabilities - 02 - Sep16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.809319) Version used: $Revision: 4189 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-7.php, http://www.php.net/ChangeLog-5.php

2.27 - PHP Multiple Vulnerabilities - 04 - Aug16 (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.808794

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.5.36

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact. Impact Level: Application

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

Vulnerability Insight
Multiple flaws are due to, - The 'get_icu_value_itable' function in 'ext/intl/locale/locale_methods.c' script does not ensure the presence of a '\0' character. - The 'gd_interpolation.c' script in the GD Graphics Library mishandled by the imagescale function.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Vulnerabilities - 04 - Aug16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808794) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php, http://www.php.net/ChangeLog-7.php

2.28 - PHP Multiple Vulnerabilities - 03 - Sep16 (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.809317

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.6.26

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, or possibly have unspecified other impact. Impact Level: Application

Solution
Upgrade to PHP version 5.6.25, or 7.0.10, or later. For updates refer to http://www.php.net

Vulnerability Insight
Multiple flaws are due to, - Use-after-free vulnerability in the 'wddx_stack_destroy' function in 'ext/wddx/wddx.c' script. - Improper varification of a BIT field has the UNSIGNED_FLAG flag in 'ext/mysqlnd/mysqlnd_wireprotocol.c' script. - The ZIP signature-verification feature does not ensure that the uncompressed_filesize field is large enough. - The script 'ext/spl/spl_array.c' proceeds with SplArray unserialization without validating a return value and data type. - The script 'ext/intl/msgformat/msgformat_format.c' does not properly restrict the locale length provided to the Locale class in the ICU library. - An error in the php_wddx_push_element function in ext/wddx/wddx.c.

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Vulnerabilities - 03 - Sep16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.809317) Version used: $Revision: 4189 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-7.php, http://www.php.net/ChangeLog-5.php

2.29 - PHP Multiple Vulnerabilities - 05 - Jul16 (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.808634

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.5.38

Impact
Successfully exploiting this issue may allow attackers to cause a denial of service obtain sensitive information from process memory, or possibly have unspecified other impact. Impact Level: Application

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

Vulnerability Insight
Multiple flaws are due to - An integer overflow in the 'php_stream_zip_opener' function in 'ext/zip/zip_stream.c' script. - An integer signedness error in the 'simplestring_addn' function in 'simplestring.c' in xmlrpc-epi. - The 'ext/snmp/snmp.c' script improperly interacts with the unserialize implementation and garbage collection. - The 'locale_accept_from_http' function in 'ext/intl/locale/locale_methods.c' script does not properly restrict calls to the ICU 'uloc_acceptLanguageFromHTTP' function. - An error in the 'exif_process_acct_comment' function in 'ext/exif/exif.c' script. - An error in the 'exif_process_IFD_in_MAKERNOTE' function in 'ext/exif/exif.c' script. - The 'ext/session/session.c' does not properly maintain a certain hash data structure. - An integer overflow in the 'virtual_file_ex' function in 'TSRM/tsrm_virtual_cwd.c' script. - An error in the 'php_url_parse_ex' function in 'ext/standard/url.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Vulnerabilities - 05 - Jul16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808634) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://php.net/ChangeLog-5.php, http://php.net/ChangeLog-7.php, http://openwall.com/lists/oss-security/2016/07/24/2

2.30 - PHP Multiple Vulnerabilities - 02 - Jan15

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.805413

Summary
This host is installed with PHP and is prone to multiple vulnerbilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result

Installed version: 5.3.10 Fixed version: 5.6.5

Impact
Successful exploitation will allow remote attackers to cause a denial of service or possibly have unspecified other impact. Impact Level: Application

Solution
Upgrade to PHP version 5.6.5 or later

Vulnerability Insight
The flaw is due to a free operation on a stack-based character array by The apprentice_load function in libmagic/apprentice.c in the Fileinfo component.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Vulnerabilities - 02 - Jan15 (OID: 1.3.6.1.4.1.25623.1.0.805413) Version used: $Revision: 3942 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
https://bugs.php.net/bug.php?id=68665, http://securitytracker.com/id/1031480

2.31 - PHP Out of Bounds Read Multiple Vulnerabilities - Jan15

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.805414

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.4.37/5.5.21/5.6.5

Impact
Successful exploitation will allow remote attackers to obtain sensitive information and trigger unexpected code execution . Impact Level: Application

Solution
Upgrade to PHP version 5.4.37 or 5.5.21 or 5.6.5 or later

Vulnerability Insight
The flaw is due to an out-of-bounds read error in sapi/cgi/cgi_main.c in the CGI component in PHP.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Out of Bounds Read Multiple Vulnerabilities - Jan15 (OID: 1.3.6.1.4.1.25623.1.0.805414) Version used: $Revision: 3942 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
https://bugs.php.net/bug.php?id=68618

2.32 - PHP Multiple Double Free Vulnerabilities - Jan15

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.805412

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.5.21/5.6.5

Impact
Successful exploitation will allow remote attackers to cause a denial of service or possibly have unspecified other impact. Impact Level: Application

Solution
Upgrade to PHP version 5.5.21 or 5.6.5 or later

Vulnerability Insight
Multiple flaws are due to: - Double free error in the 'zend_ts_hash_graceful_destroy' function in 'zend_ts_hash.c script in the Zend Engine in PHP. - flaw in the 'GetCode_' function in 'gd_gif_in.c' script in GD Graphics Library (LibGD).

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Double Free Vulnerabilities - Jan15 (OID: 1.3.6.1.4.1.25623.1.0.805412) Version used: $Revision: 3942 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://securitytracker.com/id/1031479, https://bugs.php.net/bug.php?id=68676

2.33 - Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability

H **High**: (CVSS: 7.5) 445/tcp (microsoft-ds)
OID: 1.3.6.1.4.1.25623.1.0.801991

Summary
The host is running SMB/NETBIOS and prone to authentication bypass Vulnerability

Affected Nodes
192.168.1.31(HVFS), 192.168.1.32(HVFS), 192.168.1.33(HVFS), 192.168.1.34(HVFS)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow attackers to use shares to cause the system to crash. Impact Level: System

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.

Vulnerability Insight
The flaw is due to an SMB share, allows full access to Guest accts. If the Guest account is enabled, anyone can access the computer without a valid acct account or password.

Vulnerability Detection Method
Details: Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.801991) Version used: $Revision: 3100 $

References
http://xforce.iss.net/xforce/xfdb/2, http://seclab.cs.ucdonaldson.edu/projects/testing/vulner/38.html

2.34 - PHP Remote Code Execution and Denial of Service Vulnerabilities - Dec13

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.804174

Summary
This host is installed with PHP and is prone to remote code execution vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.3.28/5.4.23/5.5.7

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption). Impact Level: Application

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

Vulnerability Insight
The flaw is due to a boundary error within the 'asn1_time_to_time_t' function in 'ext/openssl/openssl.c' when parsing X.509 certificates.

Vulnerability Detection Method
Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not. Details: PHP Remote Code Execution and Denial of Service Vulnerabilities - Dec13 (OID: 1.3.6.1.4.1.25623.1.0.804174) Version used: $Revision: 3949 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://secunia.com/advisories/56055, http://packetstormsecurity.com/files/124436/PHP-openssl_x509_parse-Memory-Corruption.html

2.35 - PHP Multiple Vulnerabilities - 01 - Mar16 (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.807503

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.4.44

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code and to create or overwrite arbitrary files on the system and this may lead to launch further attacks. Impact Level: Application

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

Vulnerability Insight
Multiple flaws are due to, - The multiple use-after-free vulnerabilities in SPL unserialize implementation. - An insufficient validation of acct supplied input by 'phar/phar_object.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Vulnerabilities - 01 - Mar16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.807503) Version used: $Revision: 4161 $

Product Detection Result

Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
https://bugs.php.net/bug.php?id=70068, http://www.openwall.com/lists/oss-security/2015/08/19/3

2.36 - PHP Multiple Vulnerabilities - 04 - Jul16 (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.808604

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.4.44

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger unintended method execution to defeat cryptographic protection mechanisms. Impact Level: Application

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

Vulnerability Insight
The multiple flaws are due to, - An improper validation of certain Exception objects in 'Zend/zend_exceptions.c' script. - The 'openssl_random_pseudo_bytes' function in 'ext/openssl/openssl.c' incorrectly relies on the deprecated 'RAND_pseudo_bytes' function.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Vulnerabilities - 04 - Jul16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808604) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php

2.37 - PHP Directory Traversal Vulnerability - Jul16 (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.808617

Summary
This host is installed with PHP and is prone to Directory traversal vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.4.45

Impact
Successfully exploiting this issue allow remote attackers to read arbitrary empty directories, also to cause a denial of service. Impact Level: Application

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

Vulnerability Insight

Multiple flaws are due to - An error in the 'ZipArchive::extractTo' function in 'ext/zip/php_zip.c' script. - The xsl_ext_function_php function in ext/xsl/xsltprocessor.c when libxml2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation after the principal argument loop. - Improper handling of multiple php_var_unserialize calls. - Multiple use-after-free vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Directory Traversal Vulnerability - Jul16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808617) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php, http://www.openwall.com/lists/oss-security/2016/03/16/20

2.38 - PHP Multiple Vulnerabilities - 03 - Jul16 (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.808603

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.5.35

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact. Impact Level: Application

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

Vulnerability Insight
The multiple flaws are due to, - An improper validation of TIFF start data in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An improper validation of IFD sizes in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An improper construction of spprintf arguments,in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An error in 'grapheme_strpos function' in 'ext/intl/grapheme/grapheme_string.c'. - An error in 'xml_parse_into_struct' function in 'ext/xml/xml.c' script. - The 'bcpowmod' function in 'ext/bcmath/bcmath.c' improperly modifies certain data structures. - An improper validation of input passed to 'bcpowmod' function in 'ext/bcmath/bcmath.c' script. - An error in 'grapheme_strpos' function in ext/intl/grapheme/grapheme_string.c script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Vulnerabilities - 03 - Jul16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808603) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php, http://www.php.net/ChangeLog-7.php

2.39 - PHP serialize_function_call Function Type Confusion Vulnerability - Mar16 (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.807505

Summary
This host is installed with PHP and is prone to remote code execution vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.4.45

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the acct running the affected application. Failed exploit attempts will likely cause a denial-of-service condition. Impact Level: Application

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

Vulnerability Insight
The flaw is due to 'SoapClient __call' method in 'ext/soap/soap.c' scripr does not properly manage headers.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 ... (OID: 1.3.6.1.4.1.25623.1.0.807505) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php, https://bugs.php.net/bug.php?id=70388

2.40 - PHP Multiple Vulnerabilities - 01 - Apr16 (Linux)

H **High**: (CVSS: 7.5)
OID: 1.3.6.1.4.1.25623.1.0.807807 — 80/tcp (http)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.5.33

Impact
Successfully exploiting this issue allow remote attackers to gain access to potentially sensitive information and conduct a denial of service (memory corruption and application crash). Impact Level: Application

Solution
Upgrade to PHP version 5.5.33 or 5.6.19 or later. For updates refer to http://www.php.net

Vulnerability Insight
Multiple flaws are due to, - A use-after-free error in wddx.c script in the WDDX extension in PHP - An error in the phar_parse_zipfile function in zip.c script in the PHAR extension in PHP.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Vulnerabilities - 01 - Apr16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.807807) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
https://bugs.php.net/bug.php?id=71587, https://bugs.php.net/bug.php?id=71498, https://secure.php.net/ChangeLog-5.php

2.41 - PHP Multiple Vulnerabilities - 01 - Jul16 (Linux)

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.808199

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.5.34

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code. Impact Level: Application

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

Vulnerability Insight
Multiple flaws are due to, - Multiple integer overflows in the mbfl_strcut function in 'ext/mbstring/libmbfl/mbfl/mbfilter.c' script. - A format string vulnerability in the php_snmp_error function in 'ext/snmp/snmp.c' script. - An improper handling of '\0' characters by the 'phar_analyze_path' function in 'ext/phar/phar.c' script. - An integer overflow in the 'php_raw_url_encode' function in 'ext/standard/url.c' script - An improper handling of continuation-level jumps in 'file_check_mem' function in 'funcs.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Vulnerabilities - 01 - Jul16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808199) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php, http://www.php.net/ChangeLog-7.php

2.42 - Report default community names of the SNMP Agent

H **High**: (CVSS: 7.5) 161/tcp (snmp)
OID: 1.3.6.1.4.1.25623.1.0.10264

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).

Affected Nodes
192.168.0.2, 192.168.0.11, 192.168.1.24, 192.168.1.205

Vulnerability Detection Result
SNMP Agent responded as expected with community name: public
Multiple results by host

Impact
If an attacker is able to guess a PUBLIC community string, they would be able to read SNMP data (depending on which MIBs are installed) from the remote device. This information might include system time, IP addresses, interfaces, processes running, etc. If an attacker is able to guess a PRIVATE community string (WRITE or 'writeall' access), they will have the ability to change information on the remote machine. This could be a huge security hole, enabling remote attackers to wreak complete havoc such as routing redi traffic, initiating processes, etc. In essence, 'writeall' access will give the remote attacker full administrative rights over the remote machine. Note that this test only gathers information and does not attempt to write to the remote device. Thus it is not possible to determine automatically whether the reported community is public or private. Also note that information made

available through a guessable community string might or might not contain sensitive data. Please review the information available through the reported community string to determine the impact of this disclosure.

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.

Vulnerability Detection Method
Details: Report default community names of the SNMP Agent (OID: 1.3.6.1.4.1.25623.1.0.10264) Version used: $Revision: 3911 $

2.43 - Lighttpd Multiple vulnerabilities

H	**High**: (CVSS: 7.5) **OID:** 1.3.6.1.4.1.25623.1.0.802072	88/tcp (kerberos)

Summary
This host is running Lighttpd and is prone to multiple vulnerabilities

Affected Nodes
192.168.0.241, 192.168.1.240

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary SQL seq and remote attackers to read arbitrary files via hostname. Impact Level: System/Application

Solution
Upgrade to 1.4.35 or higher, For updates refer to http://www.lighttpd.net/download

Vulnerability Insight
- mod_mysql_vhost module not properly sanitizing acct supplied input passed via the hostname. - mod_evhost and mod_simple_vhost modules not properly sanitizing acct supplied input via the hostname.

Vulnerability Detection Method
Send a crafted HTTP GET request and check whether it responds with error message. Details: Lighttpd Multiple vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.802072) Version used: $Revision: 3524 $

References
http://seclists.org/oss-sec/2014/q1/561, http://download.lighttpd.net/lighttpd/security/lighttpd_sa_2014_01.txt

2.44 - OpenSSH schnorr.c Remote Memory Corruption Vulnerability

H	**High**: (CVSS: 7.5) **OID:** 1.3.6.1.4.1.25623.1.0.105001	22/tcp (ssh)

Summary
OpenSSH is prone to a remote memory-corruption vulnerability.

Affected Nodes
192.168.0.3, 192.168.1.203, 192.168.1.204, 192.168.1.205

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An attacker can exploit this issue to execute arbitrary code in context of the application. Failed exploits may result in denial-of- service conditions.

Solution
Updates are available.

Vulnerability Insight
The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.

Vulnerability Detection Method
Check the version. Details: OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.105001) Version used: $Revision: 3445 $

References
http://www.securityfocus.com/bid/65230, http://www.openssh.com

2.45 - APC redi Management Card Webinterface Default Credentials

H **High**: (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.111052

Summary
The remote APC redi Management Card Webinterface is prone to a default account authentication bypass vulnerability.

Affected Nodes
192.168.1.52

Vulnerability Detection Result
It was possible to login using the following credentials: device:apc readonly:apc

Impact
This issue may be exploited by a remote attacker to gain access to sensitive information.

Solution
Change the password.

Vulnerability Insight
It was possible to login with default credentials of apc:apc, device:apc or readonly:device.

Vulnerability Detection Method
Try to login with default credentials. Details: APC redi Management Card Webinterface Default Credentials (OID: 1.3.6.1.4.1.25623.1.0.111052) Version used: $Revision: 4080 $

2.46 - APC redi Management Card Telnet Default Credentials

H **High**: (CVSS: 7.5) 23/tcp (telnet)
OID: 1.3.6.1.4.1.25623.1.0.111051

Summary
The remote APC redi Management Card has default credentials set.

Affected Nodes
192.168.1.52

Vulnerability Detection Result
It was possible to login using the following credentials: device:apc

Impact
This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.

Solution
Change/Set the password.

Vulnerability Insight
It was possible to login with default credentials of apc:apc or device:apc

Vulnerability Detection Method

Connect to the telnet service and try to login with default credentials. Details: APC redi Management Card Telnet Default Credentials (OID: 1.3.6.1.4.1.25623.1.0.111051) Version used: $Revision: 2568 $

2.47 - OpenSSH Privilege Escalation Vulnerability - May16

H **High**: (CVSS: 7.2)
OID: 1.3.6.1.4.1.25623.1.0.807574 — 22/tcp (ssh)

Summary
This host is installed with openssh and is prone to privilege escalation vulnerability.

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)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: 7.2p2-3
Multiple results by host

Impact
Successfully exploiting this issue will allow local accts to gain privileges. Impact Level: Application

Solution
Upgrade to OpenSSH version 7.2p2-3 or later. For updates refer to http://www.openssh.com

Vulnerability Insight
The flaw exists due to an error in 'do_setup_env function' in 'session.c' script in sshd which trigger a crafted environment for the /bin/login program when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in acct home directories.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: OpenSSH Privilege Escalation Vulnerability - May16 (OID: 1.3.6.1.4.1.25623.1.0.807574) Version used: $Revision: 3379 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.3 Method: SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

References
https://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-8325.html,
https://anongit.mindrot.org/openssh.git/commit/?id=85bdcd7c92fe7ff133bbc4e10a65c91810f88755

2.48 - PHP Denial of Service Vulnerability - 01 - Jul16 (Linux)

H **High**: (CVSS: 7.1)
OID: 1.3.6.1.4.1.25623.1.0.808613 — 80/tcp (http)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.5.28

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (race condition and heap memory corruption) by leveraging an application that performs many temporary-file accesses. Impact Level: Application

Solution
Upgrade to PHP version 5.5.28, or 5.6.12, or later. For updates refer to http://www.php.net

Vulnerability Insight

The flaw is due to script 'main/php_open_temporary_file.c' does not ensure thread safety.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Denial of Service Vulnerability - 01 - Jul16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808613) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php

2.49 - OpenSSH X Connections Session Hijacking Vulnerability

M **Medium**: (CVSS: 6.9) 22/tcp (ssh)
OID: 1.3.6.1.4.1.25623.1.0.100584

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.

Affected Nodes
192.168.0.3

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details: OpenSSH X Connections Session Hijacking Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.100584) Version used: $Revision: 3445 $

References
http://www.securityfocus.com/bid/28444, http://support.apple.com/kb/HT3137, http://www.openbsd.org/errata41.html, http://www.openbsd.org/errata42.html, http://www.openbsd.org/errata43.html, http://www.openssh.com/txt/release-5.0, http://www.openssh.com, http://sourceforge.net/project/shownotes.php?release_id=590180, http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011, http://www.securityfocus.com/archive/1/492447, http://aix.software.ibm.com/aix/efixes/security/ssh_advisory.asc, http://support.avaya.com/elmodocs2/security/ASA-2008-205.htm, http://www.globus.org/mail_archive/security-announce/2008/04/msg00000.html, http://support.attachmate.com/techdocs/2374.html#Security_Updates_in_7.0_SP1, http://sunsolve.sun.com/search/document.do?assetkey=1-66-237444-1

2.50 - PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux)

M **Medium**: (CVSS: 6.8) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.806649

Summary
This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed Version: 5.3.10 Fixed Version: 5.5.30

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash). Impact Level: Application

Solution
Upgrade to PHP 5.5.30 or 5.6.14 or later. For updates refer to http://www.php.net

Vulnerability Insight
Multiple flaws are due to, - An Off-by-one error in the 'phar_parse_zipfile' function within ext/phar/zip.c script. - An error in the 'phar_get_entry_data' function in ext/phar/util.c script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.806649) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php, https://bugs.php.net/bug.php?id=70433, http://www.openwall.com/lists/oss-security/2015/10/05/8

2.51 - OpenSSL CCS Man in the Middle Security Bypass Vulnerability

M **Medium**: (CVSS: 6.8) 443/tcp (https)
OID: 1.3.6.1.4.1.25623.1.0.105042

Summary
OpenSSL is prone to security-bypass vulnerability.

Affected Nodes
192.168.1.240, 192.168.6.49

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.

Solution
Updates are available.

Vulnerability Insight
OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

Vulnerability Detection Method
Send two SSL ChangeCipherSpec request and check the response. Details: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.105042) Version used: $Revision: 3599 $

References
http://www.securityfocus.com/bid/67899, http://openssl.org/

2.52 - Microsoft SQL Server Elevation of Privilege Vulnerability (2984340) - Remote

M **Medium**: (CVSS: 6.8)
OID: 1.3.6.1.4.1.25623.1.0.805110

Summary

This host is missing an important security update according to Microsoft Bulletin MS14-044.

Affected Nodes
192.168.1.16(sourcesvr), 192.168.7.99(PS01)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to cause a Denial of Service or elevation of privilege. Impact Level: Application

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

Vulnerability Insight
Flaws are due to when, - SQL Master Data Services (MDS) does not properly encode output. - SQL Server processes an incorrectly formatted T-SQL query.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: Microsoft SQL Server Elevation of Privilege Vulnerability (2984340) - Remote (OID: 1.3.6.1.4.1.25623.1.0.805110) Version used: $Revision: 3524 $

Product Detection Result
Product: cpe:/a:microsoft:sql_server:11.0.3128.0 Method: Microsoft SQL TCP/IP listener is running (OID: 1.3.6.1.4.1.25623.1.0.10144)

References
https://technet.microsoft.com/library/security/MS14-044

2.53 - PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux)

Medium: (CVSS: 6.8)
OID: 1.3.6.1.4.1.25623.1.0.808609

80/tcp (http)

Summary
This host is installed with PHP and is prone to denial of service and unspecified Vulnerabilities

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.6.18

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact. Impact Level: Application

Solution
Upgrade to PHP version 5.6.18, or 7.0.3, or later. For updates refer to http://www.php.net

Vulnerability Insight
The flaw is due an improper handling of zero-size './/@LongLink' files by 'phar_make_dirstream' function in ext/phar/dirstream.c script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808609) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References

http://www.php.net/ChangeLog-5.php, http://www.openwall.com/lists/oss-security/2016/04/28/2

2.54 - VMSA-2016-0002: VMware product updates address a critical glibc security vulnerability (remote check)

M **Medium**: (CVSS: 6.8)
OID: 1.3.6.1.4.1.25623.1.0.105561

Summary
VMware product updates address a critical glibc security vulnerability

Affected Nodes
192.168.6.154

Vulnerability Detection Result
ESXi Version: 5.5.0 Detected Build: 2403361 Fixed Build: 3568722

Solution
Apply the missing patch(es).

Vulnerability Insight
a. glibc update for multiple products. The glibc library has been updated in multiple products to resolve a stack buffer overflow present in the glibc getaddrinfo function.

Vulnerability Detection Method
Check the build number Details: VMSA-2016-0002: VMware product updates address a critical glibc security vul... (OID: 1.3.6.1.4.1.25623.1.0.105561) Version used: $Revision: 2717 $

References
http://www.vmware.com/security/advisories/VMSA-2016-0002.html

2.55 - OpenSSL DSA_verify() Security Bypass Vulnerability in BIND

M **Medium**: (CVSS: 6.8)
OID: 1.3.6.1.4.1.25623.1.0.800338
53/udp (domain)

Summary
The host is running BIND and is prone to Security Bypass Vulnerability.

Affected Nodes
192.168.3.2

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow remote attackers to bypass the certificate validation checks and can cause man-in-the-middle attack via signature checks on DSA and ECDSA codes used with SSL/TLS. Impact Level: Application

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

Vulnerability Insight
The flaw is due to improper validation of return value from OpenSSL's DSA_do_verify and VP_VerifyFinal functions.

Vulnerability Detection Method
Details: OpenSSL DSA_verify() Security Bypass Vulnerability in BIND (OID: 1.3.6.1.4.1.25623.1.0.800338) Version used: $Revision: 3386 $

References
https://www.isc.org/node/373, http://secunia.com/advisories/33404/, http://www.ocert.org/advisories/ocert-2008-016.html

2.56 - Samba libcli/smb/smbXcli_base.c Man In The Middle (MIMA) Vulnerability

Medium: (CVSS: 6.8)
OID: 1.3.6.1.4.1.25623.1.0.807345
445/tcp (microsoft-ds)

Summary
This host is running Samba and is prone to man-in-the-middle vulnerability.

Affected Nodes
192.168.6.82(MINTLINUX)

Vulnerability Detection Result
Installed version: 4.1.6 Fixed version: 4.2.14

Impact
Successful exploitation will allow a remote attacker to bypass a client-signing protection mechanism, and consequently spoof SMB2 and SMB3 servers. Impact Level: Application

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

Vulnerability Insight
The flaw exists in the way DCE/RPC connections are initiated by the acct. Any authenticated DCE/RPC connection that a client initiates against the server could be use by a man-in-the middle attacker to impersonate the server by injecting the SMB2_SESSION_FLAG_IS_GUEST or SMB2_SESSION_FLAG_IS_NULL flag.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: Samba 'libcli/smb/smbXcli_base.c' Man In The Middle (MIMA) Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.807345) Version used: $Revision: 3698 $

Product Detection Result
Product: cpe:/a:samba:samba:4.1.6 Method: SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

References
https://www.samba.org/samba/security/CVE-2016-2119.html, https://access.redhat.com/security/cve/cve-2016-2119

2.57 - Samba Badlock Critical Vulnerability

Medium: (CVSS: 6.8)
OID: 1.3.6.1.4.1.25623.1.0.807646
445/tcp (microsoft-ds)

Summary
This host is running Samba and is prone to badlock vulnerability.

Affected Nodes
192.168.1.50(myco-bdr), 192.168.6.82(MINTLINUX)

Vulnerability Detection Result
Installed version: 3.6.3 Fixed version: 4.2.11 or 4.3.8 or 4.4.2, or later
Multiple results by host

Impact
Successful exploitation of this vulnerability leads to Man-in-the-middle (MITM) attacks, to causes denial of service, to spoof and to obtain sensitive session information. Impact Level: Application

Solution
Upgrade to samba version 4.2.11, or 4.3.8, or 4.4.2, or later.

Vulnerability Insight
The multiple flaws are due to - The Multiple errors in DCE-RPC code. - A spoofing Vulnerability in NETLOGON. - The LDAP implementation did not enforce integrity protection for LDAP connections. - The SSL/TLS certificates

are not validated in certain connections. - Not enforcing Server Message Block (SMB) signing for clients using the SMB1 protocol. - An integrity protection for IPC traffic is not enabled by default - The MS-SAMR and MS-LSAD protocol implementations mishandle DCERPC connections. - An error in the implementation of NTLMSSP authentication. -

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: Samba Badlock Critical Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.807646) Version used: $Revision: 3901 $

Product Detection Result
Product: cpe:/a:samba:samba:3.6.3 Method: SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

References
http://badlock.org/, http://thehackernews.com/2016/03/windows-samba-vulnerability.html

2.58 - PHP XML Entity Expansion And XML External Entity Vulnerabilities (Linux)

Medium: (CVSS: 6.8)
OID: 1.3.6.1.4.1.25623.1.0.808615

80/tcp (http)

Summary
This host is installed with PHP and is prone to XML entity expansion and XML external entity vulnerbilities

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.5.22

Impact
Successfully exploiting this issue allow remote attackers to conduct XML External Entity (XXE) and XML Entity Expansion (XEE) attacks. Impact Level: Application

Solution
Upgrade to PHP version 5.5.22, or 5.6.6, or later. For updates refer to http://www.php.net

Vulnerability Insight
The flaw is due to script 'ext/libxml/libxml.c' does not isolate each thread from 'libxml_disable_entity_loader' when PHP-FPM is used.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP XML Entity Expansion And XML External Entity Vulnerabilities (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808615) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php

2.59 - VMSA-2016-0001 VMware ESXi, Fusion, Player, and Workstation updates address important guest privilege escalation vulnerability (remote check)

Medium: (CVSS: 6.5)
OID: 1.3.6.1.4.1.25623.1.0.105509

Summary
VMware ESXi, Fusion, Player, and Workstation updates address important guest privilege escalation vulnerability

Affected Nodes
192.168.6.154

Vulnerability Detection Result
ESXi Version: 5.5.0 Detected Build: 2403361 Fixed Build: 3247226

Solution
Apply the missing patch(es).

Vulnerability Insight
Important Windows-based guest privilege escalation in VMware Tools A kernel memory corruption vulnerability is present in the VMware Tools 'Shared Folders' (HGFS) feature running on Microsoft Windows. Successful exploitation of this issue could lead to an escalation of privilege in the guest operating system.

Vulnerability Detection Method
Check the build number Details: VMSA-2016-0001 VMware ESXi, Fusion, Player, and Workstation updates address ... (OID: 1.3.6.1.4.1.25623.1.0.105509) Version used: $Revision: 2478 $

References
http://www.vmware.com/security/advisories/VMSA-2016-0001.html

2.60 - PHP Denial of Service Vulnerability - 02 - Aug16 (Linux)

Medium: (CVSS: 6.4)
OID: 1.3.6.1.4.1.25623.1.0.809139
80/tcp (http)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.5.31

Impact
Successfully exploiting this issue allow attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read and buffer overflow) via a long string. Impact Level: Application

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

Vulnerability Insight
The flaw is due to the 'sapi/fpm/fpm/fpm_log.c' script misinterprets the semantics of the snprintf return value.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Denial of Service Vulnerability - 02 - Aug16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.809139) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php

2.61 - PHP make_http_soap_request Information Disclosure Vulnerability (Linux)

Medium: (CVSS: 6.4)
OID: 1.3.6.1.4.1.25623.1.0.808666
80/tcp (http)

Summary
This host is installed with PHP and is prone to denial of service or information disclosure vulnerabilities

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.4.44

Impact
Successfully exploiting this issue allow remote attackers to obtain sensitive information from process memory or cause a denial of service. Impact Level: Application

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

Vulnerability Insight
The flaw is due an error in the 'make_http_soap_request' function in 'ext/soap/php_http.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP 'make_http_soap_request' Information Disclosure Vulnerability (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808666) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php, http://www.php.net/ChangeLog-7.php

2.62 - PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Linux)

M **Medium**: (CVSS: 6.4)
OID: 1.3.6.1.4.1.25623.1.0.807504 — 80/tcp (http)

Summary
This host is installed with PHP and is prone to out-of-bounds read memory corruption vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.5.31

Impact
Successfully exploiting this issue allow remote attackers to obtain sensitive information or cause a denial-of-service condition. Impact Level: Application

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

Vulnerability Insight
The flaw is due to memory corruption vulnerability via a large 'bgd_color' argument to the 'imagerotate' function in 'ext/gd/libgd/gd_interpolation.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.807504) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
https://bugs.php.net/bug.php?id=70976, http://www.openwall.com/lists/oss-security/2016/01/14/8

2.63 - Microsoft Windows SMTP Server DNS spoofing vulnerability

M **Medium**: (CVSS: 6.4)
OID: 1.3.6.1.4.1.25623.1.0.100624 — 25/tcp (smtp)

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.

Affected Nodes
192.168.7.68(REMOTE)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
This issue is reported to be patched in Microsoft security advisory MS10-024 please see the references for more information.

Vulnerability Detection Method
Details: Microsoft Windows SMTP Server DNS spoofing vulnerability (OID: 1.3.6.1.4.1.25623.1.0.100624) Version used: $Revision: 3152 $

References
http://www.securityfocus.com/bid/39910, http://www.securityfocus.com/bid/39908, http://archives.neohapsis.com/archives/fulldisclosure/2010-05/0058.html, http://www.microsoft.com, http://www.coresecurity.com/content/CORE-2010-0424-windows-stmp-dns-query-id-bugs, http://www.microsoft.com/technet/security/Bulletin/MS10-024.mspx

2.64 - PHP Directory Traversal Vulnerability

Medium: (CVSS: 5.8)
OID: 1.3.6.1.4.1.25623.1.0.103486

80/tcp (http)

Summary
PHP is prone to a directory-traversal vulnerability because it fails to properly sanitize acct-supplied input.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.3.10/5.4.1

Impact
Exploiting this issue may allow an attacker to retrieve, corrupt or upload arbitrary files at arbitrary locations that could aid in further attacks.

Solution
Updates are available. Please see the references for more information.

Vulnerability Insight
Remote attackers can use specially crafted requests with directory- traversal sequences ('../') to retrieve, corrupt or upload arbitrary files in the context of the application.

Vulnerability Detection Method
Details: PHP Directory Traversal Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103486) Version used: $Revision: 3973 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.securityfocus.com/bid/53403, https://bugzilla.redhat.com/show_bug.cgi?id=799187, http://www.php.net/archive/2012.php#id2012-04-26-1, http://www.php.net/

2.65 - OpenSSH child_set_env() Function Security Bypass Vulnerability

Medium: (CVSS: 5.8)
OID: 1.3.6.1.4.1.25623.1.0.105003

22/tcp (ssh)

Summary
OpenSSH is prone to a security-bypass vulnerability.

Affected Nodes
192.168.0.3, 192.168.1.203, 192.168.1.204, 192.168.1.205

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
The security bypass allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.

Solution
Updates are available.

Vulnerability Insight
sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config.

Vulnerability Detection Method
Check the version. Details: OpenSSH 'child_set_env()' Function Security Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.105003) Version used: $Revision: 3445 $

References
http://www.securityfocus.com/bid/66355, http://www.openssh.com

2.66 - OpenSSH Certificate Validation Security Bypass Vulnerability

Medium: (CVSS: 5.8)
OID: 1.3.6.1.4.1.25623.1.0.105004

22/tcp (ssh)

Summary
OpenSSH is prone to a security-bypass vulnerability.

Affected Nodes
192.168.0.3, 192.168.1.203, 192.168.1.204, 192.168.1.205

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Attackers can exploit this issue to bypass certain security restrictions and perform unauthorized actions. This may aid in further attacks.

Solution
Updates are available.

Vulnerability Insight
The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.

Vulnerability Detection Method
Check the version Details: OpenSSH Certificate Validation Security Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.105004) Version used: $Revision: 3445 $

References
http://www.securityfocus.com/bid/66459, http://www.openssh.com

2.67 - OpenSSH <= 7.2p1 - Xauth Injection

Medium: (CVSS: 5.5)
OID: 1.3.6.1.4.1.25623.1.0.105581

22/tcp (ssh)

Summary

openssh xauth dbre injection may lead to forced-dbre and /bin/false bypass

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)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: 7.2p2
Multiple results by host

Impact
By injecting xauth seq one gains limited* read/write arbitrary files, information leakage or xauth-connect capabilities.

Solution
Upgrade to OpenSSH version 7.2p2 or later. For updates refer to http://www.openssh.com

Vulnerability Insight
An authenticated acct may inject arbitrary xauth seq by sending an x11 channel request that includes a newline character in the x11 cookie. The newline acts as a dbre separator to the xauth binary. This attack requires the server to have 'X11Forwarding yes' enabled. Disabling it, mitigates this vector.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: OpenSSH <= 7.2p1 - Xauth Injection (OID: 1.3.6.1.4.1.25623.1.0.105581) Version used: $Revision: 2970 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.3 Method: SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

References
http://www.openssh.com/txt/release-7.2p2

2.68 - Dropbear SSH CRLF Injection Vulnerability

M	**Medium**: (CVSS: 5.5) **OID:** 1.3.6.1.4.1.25623.1.0.807740	22/tcp (ssh)

Summary
This host is installed with dropbear ssh and is prone to crlf injection vulnerability.

Affected Nodes
192.168.0.11, 192.168.1.240, 192.168.6.49

Vulnerability Detection Result
Installed version: 2014.63 Fixed version: 2016.72
Multiple results by host

Impact
Successfully exploiting this issue allow remote authenticated accts to inject seq to xauth.. Impact Level: Application

Solution
Upgrade to Dropbear SSH version 2016.72 or later. For updates refer to http://www.openssh.com

Vulnerability Insight
The flaw exists due to invalid processing of 'X11' forwarding input.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: Dropbear SSH CRLF Injection Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.807740) Version used: $Revision: 3000 $

Product Detection Result
Product: cpe:/a:matt_jonston:dropbear_ssh_server:2014.63 Method: Dropbear SSH Detection (OID: 1.3.6.1.4.1.25623.1.0.105112)

References
https://github.com/tintinweb/pub/tree/master/pocs/cve-2016-3116

2.69 - PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux)

M	**Medium**: (CVSS: 5.1) **OID:** 1.3.6.1.4.1.25623.1.0.808628	80/tcp (http)

Summary
This host is installed with PHP and is prone to Man-in-the-middle attack vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 7.0.9

Impact
Successfully exploiting this issue may allow remote, unauthenticated to conduct MITM attacks on itable server subrequests or direct the server to initiate connections to arbitrary hosts or to cause a denial of service. Impact Level: Application

Solution
Upgrade to PHP version 7.0.9 or later. For updates refer to http://www.php.net

Vulnerability Insight
The web servers running in a CGI or CGI-like context may assign client request Proxy header values to itable HTTP_PROXY environment variables and 'HTTP_PROXY' is improperly trusted by some PHP libraries and applications and flaw exist in the gdImageCropThreshold function in 'gd_crop.c' in the GD Graphics Library.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808628) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.kb.cert.org/vuls/id/797896, https://bugs.php.net/bug.php?id=72573, https://bugs.php.net/bug.php?id=72494

2.70 - IPMI MD2 Auth Type Support Enabled

M	**Medium**: (CVSS: 5.1) **OID:** 1.3.6.1.4.1.25623.1.0.103839	623/udp (asf-rmcp)

Summary
IPMI MD2 auth type support is enabled on the remote host.

Affected Nodes
192.168.1.201, 192.168.1.202, 192.168.1.203, 192.168.1.204, 192.168.1.205

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Disable MD2 auth type support.

Vulnerability Detection Method
Details: IPMI MD2 Auth Type Support Enabled (OID: 1.3.6.1.4.1.25623.1.0.103839) Version used: $Revision: 2939 $

2.71 - LDAP allows null bases

M	**Medium**: (CVSS: 5) **OID:** 1.3.6.1.4.1.25623.1.0.10722	389/tcp (ldap)

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'

Affected Nodes
192.168.1.3(DC03), 192.168.1.4, 192.168.1.23

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Disable NULL BASE queries on your LDAP server

Vulnerability Detection Method
Details: LDAP allows null bases (OID: 1.3.6.1.4.1.25623.1.0.10722) Version used: $Revision: 2442 $

2.72 - TCP Sequence Number Approximation Reset Denial of Service Vulnerability

M **Medium**: (CVSS: 5)
OID: 1.3.6.1.4.1.25623.1.0.902815

Summary
The host is running TCP services and is prone to denial of service vulnerability.

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

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to guess sequence numbers and cause a denial of service to persistent TCP connections by repeatedly injecting a TCP RST packet.

Solution
Please see the referenced advisories for more information on obtaining and applying fixes.

Vulnerability Insight
The flaw is triggered when spoofed TCP Reset packets are received by the targeted TCP stack and will result in loss of availability for the attacked TCP services.

Vulnerability Detection Method
A TCP Reset packet with a different sequence number is sent to the target. A previously open connection is then checked to see if the target closed it or not. Details: TCP Sequence Number Approximation Reset Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902815) Version used: $Revision: 4048 $

References
http://xforce.iss.net/xforce/xfdb/15886, http://www.us-cert.gov/cas/techalerts/TA04-111A.html, http://www-01.ibm.com/support/docview.wss?uid=isg1IY55949, http://www-01.ibm.com/support/docview.wss?uid=isg1IY55950, http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006, http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx, http://www.microsoft.com/technet/security/bulletin/ms06-064.mspx, http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html, http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html

2.73 - Missing httpOnly Cookie Attribute

M **Medium**: (CVSS: 5)
OID: 1.3.6.1.4.1.25623.1.0.105925 80/tcp (http)

Summary
The application is missing the 'httpOnly' cookie attribute

Affected Nodes
192.168.1.1, 192.168.5.1

Vulnerability Detection Result
The cookies: Set-Cookie: session=; path=/;   are missing the httpOnly attribute.

Impact
Application

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

Vulnerability Insight
The flaw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Vulnerability Detection Method
Check all cookies sent by the application for a missing 'httpOnly' attribute Details: Missing httpOnly Cookie Attribute (OID: 1.3.6.1.4.1.25623.1.0.105925) Version used: $Revision: 2826 $

References
https://www.owasp.org/index.php/HttpOnly, https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)

2.74 - OpenSSH Denial of Service Vulnerability

Medium: (CVSS: 5)
OID: 1.3.6.1.4.1.25623.1.0.103939

22/tcp (ssh)

Summary
OpenSSH is prone to a remote denial-of-service vulnerability.

Affected Nodes
192.168.0.3, 192.168.1.203, 192.168.1.204, 192.168.1.205

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Exploiting this issue allows remote attackers to trigger denial-of- service conditions.

Solution
Updates are available.

Vulnerability Insight
The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.

Vulnerability Detection Method
Compare the version retrieved from the banner with the affected range. Details: OpenSSH Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103939) Version used: $Revision: 3445 $

References
http://www.securityfocus.com/bid/58162, http://www.openssh.com

2.75 - Use LDAP search request to retrieve information from NT Directory Services

Medium: (CVSS: 5)
OID: 1.3.6.1.4.1.25623.1.0.12105

389/tcp (ldap)

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.

Affected Nodes
192.168.1.3(DC03), 192.168.1.4, 192.168.1.23

Vulnerability Detection Result
The following information was pulled from the server via a LDAP request: NTDS Settings,CN=DC03,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=Corp,DC=myco,DC=com

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

Vulnerability Detection Method
Details: Use LDAP search request to retrieve information from NT Directory Services (OID: 1.3.6.1.4.1.25623.1.0.12105) Version used: $Revision: 3398 $

2.76 - OpenSSH Denial of Service Vulnerability - Jan16

Summary
This host is installed with openssh and is prone to denial of service vulnerability.

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)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: 7.1p2
Multiple results by host

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read and application crash). Impact Level: Application

Solution
Upgrade to OpenSSH version 7.1p2 or later. For updates refer to http://www.openssh.com

Vulnerability Insight
The flaw exists due to an error in 'ssh_packet_read_poll2' function within 'packet.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: OpenSSH Denial of Service Vulnerability - Jan16 (OID: 1.3.6.1.4.1.25623.1.0.806671) Version used: $Revision: 2534 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.3 Method: SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

References
http://www.openssh.com/txt/release-7.1p2,
https://anongit.mindrot.org/openssh.git/commit/?id=2fecfd486bdba9f51b3a789277bb0733ca36e1c0

2.77 - SNMP GETBULK Reflected DrDoS

Summary
The remote SNMP daemon allows distributed reflection and amplification (DrDoS) attacks

Affected Nodes
192.168.0.2, 192.168.1.24

Vulnerability Detection Result
By sending a SNMP GetBulk request of 41 bytes, we received a response of 1284 bytes.
Multiple results by host

Impact
Successfully exploiting this vulnerability allows attackers to cause denial-of-service conditions against remote hosts

Solution
Disable the SNMP service on the remote host if you do not use it or restrict access to this service

Vulnerability Detection Method
Send a SNMP GetBulk request and check the response Details: SNMP GETBULK Reflected DrDoS (OID: 1.3.6.1.4.1.25623.1.0.105062) Version used: $Revision: 2827 $

References
http://www.darkreading.com/attacks-breaches/snmp-ddos-attacks-spike/d/d-id/1269149

2.78 - Lighttpd http_auth.c Remote Code Execution Vulnerability - June15 (Linux)

M	**Medium**: (CVSS: 5) **OID:** 1.3.6.1.4.1.25623.1.0.805593	88/tcp (kerberos)

Summary
This host is running Lighttpd and is prone to remote code execution vulnerability.

Affected Nodes
192.168.0.241, 192.168.0.242, 192.168.1.240

Vulnerability Detection Result
Installed version: 1.4.31 Fixed version: 1.4.36
Multiple results by host

Impact
Successful exploitation will allows a remote attacker to execute arbitrary code on affected system. Impact Level: System/Application

Solution
Upgrade to Lighttpd 1.4.36 or later, For updates refer to to http://www.lighttpd.net

Vulnerability Insight
The flaw exists due to an error in 'http_auth.c' which does not properly validate acct-supplied input.

Vulnerability Detection Method
Check if the vulnerable version of Lighttpd is installed or not. Details: Lighttpd 'http_auth.c' Remote Code Execution Vulnerability - June15 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.805593) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:lighttpd:lighttpd:1.4.31 Method: Lighttpd Server Detection (OID: 1.3.6.1.4.1.25623.1.0.111079)

References
http://www.securitytracker.com/id/1032405, http://jaanuskp.blogspot.in/2015/05/cve-2015-3200.html

2.79 - DCE Services Enumeration

M	**Medium**: (CVSS: 5) **OID:** 1.3.6.1.4.1.25623.1.0.10736	135/tcp (loc-srv)

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.

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)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.
Multiple results by host

Solution
filter incoming traffic to this port.

Vulnerability Detection Method
Details: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736) Version used: $Revision: 2837 $

2.80 - Check for SSL Weak Ciphers

Medium: (CVSS: 5)
OID: 1.3.6.1.4.1.25623.1.0.103440

443/tcp (https)

Summary
This routine search for weak SSL ciphers offered by a service.

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), 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)

Vulnerability Detection Result
Weak ciphers offered by this service: TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_SHA TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA
Multiple results by host

Solution
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength: - Any SSL/TLS using no cipher is considered weak. - All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol. - RC4 is considered to be weak. - 64-bit block cipher 3DES vulnerable to SWEET32 attack(CVE-2016-2183). - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak. - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong

Vulnerability Detection Method
Details: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440) Version used: $Revision: 4166 $

References
https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html

2.81 - PHP Fileinfo Component Denial of Service Vulnerability (Linux)

M **Medium**: (CVSS: 5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.808669

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.6.0

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service. Impact Level: Application

Solution
Upgrade to PHP version 5.6.0 For updates refer to http://www.php.net

Vulnerability Insight
The flaw is due an improper validation of input to zero root_storage value in a CDF file.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Fileinfo Component Denial of Service Vulnerability (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808669) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php

2.82 - PHP Multiple Denial of Service Vulnerabilities (Linux)

M **Medium**: (CVSS: 5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.808611

Summary
This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.6.12

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (application crash or memory consuption). Impact Level: Application

Solution
Upgrade to PHP version 5.6.12 or later. For updates refer to http://www.php.net

Vulnerability Insight
Multiple flaws are due to - An improper handling of driver behavior for SQL_WVARCHAR columns in the 'odbc_bindcols function' in 'ext/odbc/php_odbc.c' script. - The 'gdImageScaleTwoPass' function in gd_interpolation.c script in the GD Graphics Library uses inconsistent allocate and free approaches.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Multiple Denial of Service Vulnerabilities (Linux) (OID: 1.3.6.1.4.1.25623.1.0.808611) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php

2.83 - PHP CDF File Parsing Denial of Service Vulnerabilities - 01 - Jun14

M **Medium**: (CVSS: 5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.804639

Summary
This host is installed with PHP and is prone to denial of service vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.4.29/5.5.13

Impact
Successful exploitation will allow remote attackers to conduct denial of service attacks. Impact Level: Application

Solution
Upgrade to PHP version 5.4.29 or 5.5.13 or later. For updates refer to http://php.net

Vulnerability Insight
The flaw is due to - An error due to an infinite loop within the 'unpack_summary_info' function in src/cdf.c script. - An error within the 'cdf_read_property_info' function in src/cdf.c script.

Vulnerability Detection Method
Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not. Details: PHP CDF File Parsing Denial of Service Vulnerabilities - 01 - Jun14 (OID: 1.3.6.1.4.1.25623.1.0.804639) Version used: $Revision: 3942 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://www.php.net/ChangeLog-5.php, http://secunia.com/advisories/58804, https://www.hkcert.org/my_url/en/alert/14060401

2.84 - Quote of the day

Medium: (CVSS: 5)
OID: 1.3.6.1.4.1.25623.1.0.10198
17/tcp (qotd)

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.

Affected Nodes
192.168.7.68(REMOTE)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

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.

Vulnerability Detection Method
Details: Quote of the day (OID: 1.3.6.1.4.1.25623.1.0.10198) Version used: $Revision: 3362 $

2.85 - Dropbear SSH Server Multiple Security Vulnerabilities

Medium: (CVSS: 5)
OID: 1.3.6.1.4.1.25623.1.0.105114
22/tcp (ssh)

Summary
This host is installed with Dropbear SSH Server and is prone to multiple vulnerabilities.

Affected Nodes
192.168.1.240

Vulnerability Detection Result
Installed version: 2013.58 Fixed version: 2013.59

Impact
The flaws allows remote attackers to cause a denial of service or to discover valid acctnames.

Solution
Updates are available.

Vulnerability Insight
Multiple flaws are due to, - The buf_decompress function in packet.c in Dropbear SSH Server before 2013.59 allows remote attackers to cause a denial of service (memory consumption) via a compressed packet that has a large size when it is decompressed. - Dropbear SSH Server before 2013.59 generates error messages for a failed logon attempt with different time delays depending on whether the acct account exists.

Vulnerability Detection Method
Check the version. Details: Dropbear SSH Server Multiple Security Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.105114) Version used: $Revision: 2827 $

Product Detection Result
Product: cpe:/a:matt_jonston:dropbear_ssh_server:2013.58 Method: Dropbear SSH Detection (OID: 1.3.6.1.4.1.25623.1.0.105112)

References
http://www.securityfocus.com/bid/62958, http://www.securityfocus.com/bid/62993, https://matt.ucc.asn.au/dropbear/dropbear.html

2.86 - Chargen

M	**Medium**: (CVSS: 5) **OID:** 1.3.6.1.4.1.25623.1.0.10043	19/udp (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 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.

Affected Nodes
192.168.7.68(REMOTE)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

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.

Vulnerability Detection Method
Details: Chargen (OID: 1.3.6.1.4.1.25623.1.0.10043) Version used: $Revision: 3395 $

2.87 - PHP open_basedir Security Bypass Vulnerability

M	**Medium**: (CVSS: 5) **OID:** 1.3.6.1.4.1.25623.1.0.804241	80/tcp (http)

Summary
This host is installed with PHP and is prone to security bypass vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: N/A

Impact
Successful exploitation will allow remote attackers to read arbitrary files. Impact Level: Application

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.

Vulnerability Insight
The flaw is in libxml RSHUTDOWN function which allows to bypass open_basedir protection mechanism through stream_close method call.

Vulnerability Detection Method

Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not. Details: PHP 'open_basedir' Security Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.804241) Version used: $Revision: 3942 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
https://bugzilla.redhat.com/show_bug.cgi?id=802591

2.88 - Microsoft IIS Default Welcome Page Information Disclosure Vulnerability

Medium: (CVSS: 5)
OID: 1.3.6.1.4.1.25623.1.0.802806
80/tcp (http)

Summary
The host is running Microsoft IIS Webserver and is prone to information disclosure vulnerability.

Affected Nodes
192.168.1.21, 192.168.1.69, 192.168.1.81, 192.168.6.142(QB01)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to obtain sensitive information that could aid in further attacks. Impact Level: Application

Solution
Disable the default pages within the server configuration.

Vulnerability Insight
The flaw is due to misconfiguration of IIS Server, which allows to access default pages when the server is not used.

Vulnerability Detection Method
Details: Microsoft IIS Default Welcome Page Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802806) Version used: $Revision: 2715 $

References
http://www.iis.net/

2.89 - Microsoft Windows SMTP Server MX Record Denial of Service Vulnerability

Medium: (CVSS: 5)
OID: 1.3.6.1.4.1.25623.1.0.100596
25/tcp (smtp)

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.

Affected Nodes
192.168.7.68(REMOTE)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Microsoft released fixes to address this issue. Please see the references for more information.

Vulnerability Detection Method
Details: Microsoft Windows SMTP Server MX Record Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.100596) Version used: $Revision: 3152 $

References
http://www.securityfocus.com/bid/39308, http://www.securityfocus.com/bid/39381, http://www.microsoft.com, http://support.avaya.com/css/P8/documents/100079218, http://www.microsoft.com/technet/security/Bulletin/MS10-024.mspx

2.90 - SSL Certification Expired

Medium: (CVSS: 5)
OID: 1.3.6.1.4.1.25623.1.0.103955
443/tcp (https)

Summary
The remote server's SSL certificate has already expired.

Affected Nodes
192.168.1.15(UTIL12), 192.168.1.69, 192.168.1.81, 192.168.6.5, 192.168.6.142(QB01)

Vulnerability Detection Result
Expired Certificates: The SSL certificate on the remote service expired on 2015-03-05 03:11:12 Certificate details: subject ...: CN=Gateway.myco.com issued by .: CN=Gateway.myco.com serial ....: 2086FE754DC1F38649F9B87D68B010D3 valid from : 2014-03-05 02:51:12 UTC valid until: 2015-03-05 03:11:12 UTC fingerprint: ED9280BA7FE719F2FA9B2D056585B6BFA06AA68E
Multiple results by host

Solution
Replace the SSL certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: SSL Certification Expired (OID: 1.3.6.1.4.1.25623.1.0.103955) Version used: $Revision: 3955 $

2.91 - Samba Denial of Service Vulnerability

Medium: (CVSS: 4.9)
OID: 1.3.6.1.4.1.25623.1.0.807710
445/tcp (microsoft-ds)

Summary
This host is running Samba and is prone to denial of service vulnerability.

Affected Nodes
192.168.6.82(MINTLINUX)

Vulnerability Detection Result
Installed version: 4.1.6 Fixed version: 4.1.23

Impact
Successful exploitation will allow a remote attacker to cause denial of service. Impact Level: Application

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/

Vulnerability Insight
The flaw exist due to an error in AD DC configuration in the itable DNS server.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: Samba Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.807710) Version used: $Revision: 3000 $

Product Detection Result
Product: cpe:/a:samba:samba:4.1.6 Method: SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

References
https://www.samba.org/samba/security/CVE-2016-0771.html

2.92 - OpenSSH Client Information Leak

Medium: (CVSS: 4.6)
OID: 1.3.6.1.4.1.25623.1.0.105512
22/tcp (ssh)

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.

Affected Nodes
192.168.1.24, 192.168.1.201, 192.168.1.202, 192.168.6.82(MINTLINUX)

Vulnerability Detection Result
Installed version: 6.6.1p1 Fixed version: 7.1p2
Multiple results by host

Solution
Update to 7.1p or newer.

Vulnerability Detection Method
Check the version from ssh-banner. Details: OpenSSH Client Information Leak (OID: 1.3.6.1.4.1.25623.1.0.105512) Version used: $Revision: 4052 $

References
http://www.openssh.com/txt/release-7.1p2

2.93 - PHP display_errors Cross Site Scripting Vulnerability

Medium: (CVSS: 4.3)
OID: 1.3.6.1.4.1.25623.1.0.803778
80/tcp (http)

Summary
This host is installed with PHP and is prone to cross site scripting vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.3.11/5.4.1

Impact
Successful exploitation will allow remote attackers to insert arbitrary HTML and script code, which will be executed in a acct's browser session in the context of an affected site. Impact Level: Application

Solution
Upgrade to latest version of PHP, http://www.php.net/downloads.php

Vulnerability Insight
The flaw is due to an error in handling 'display_errors', when display_errors is set to on and html_errors is set to on.

Vulnerability Detection Method
Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not. Details: PHP 'display_errors' Cross Site Scripting Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.803778) Version used: $Revision: 3942 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://packetstormsecurity.com/files/111695/, http://dl.packetstormsecurity.net/1204-exploits/php-xss.txt

2.94 - SSH Weak Encryption Algorithms Supported

M **Medium**: (CVSS: 4.3)
OID: 1.3.6.1.4.1.25623.1.0.105611 — 22/tcp (ssh)

Summary
The remote SSH server is configured to allow 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

Vulnerability Detection Result
The following weak client-to-server encryption algorithms are supported by the remote service: aes128-cbc 3des-cbc blowfish-cbc cast128-cbc arcfour128 arcfour256 arcfour aes192-cbc aes256-cbc rijndael-cbc@lysator.liu.se
The following weak server-to-client encryption algorithms are supported by the remote service: aes128-cbc 3des-cbc blowfish-cbc cast128-cbc arcfour128 arcfour256 arcfour aes192-cbc aes256-cbc rijndael-cbc@lysator.liu.se
Multiple results by host

Solution
Disable the weak encryption algorithms.

Vulnerability Insight
The `arcfour` cipher is the Arcfour stream cipher with 128-bit codes. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak codes, and should not be used anymore. The `none` algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it. A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Check if remote ssh service supports Arcfour, none or CBC ciphers. Details: SSH Weak Encryption Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105611) Version used: $Revision: 3160 $

References
https://tools.ietf.org/html/rfc4253#section-6.3, https://www.kb.cert.org/vuls/id/958563

2.95 - OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (FREAK)

M **Medium**: (CVSS: 4.3)
OID: 1.3.6.1.4.1.25623.1.0.805142 — 443/tcp (https)

Summary
This host is installed with OpenSSL and is prone to man in the middle attack.

Affected Nodes
192.168.1.201, 192.168.1.202, 192.168.1.203

Vulnerability Detection Result
EXPORT_RSA cipher suites supported by the remote server: TLSv1.0: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0014) TLSv1.0: TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0008) TLSv1.0: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0006) TLSv1.0: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0003) TLSv1.1: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0014) TLSv1.1: TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0008) TLSv1.1: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5

(0006) TLSv1.1: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0003) TLSv1.2: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0014) TLSv1.2: TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0008) TLSv1.2: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0006) TLSv1.2: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0003)
Multiple results by host

Impact
Successful exploitation will allow remote attacker to downgrade the security of a session to use EXPORT_RSA ciphers, which are significantly weaker than non-export ciphers. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream. Impact Level: Application

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

Vulnerability Insight
Flaw is due to improper handling RSA temporary codes in a non-export RSA key exchange ciphersuite.

Vulnerability Detection Method
Send a crafted 'Client Hello' request and check the servers response. Details: OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (FREAK) (OID: 1.3.6.1.4.1.25623.1.0.805142) Version used: $Revision: 4098 $

References
https://freakattack.com, http://secpod.org/blog/?p=3818, http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html

2.96 - OpenSSL TLS DHE_EXPORT LogJam Man in the Middle Security Bypass Vulnerability

Medium: (CVSS: 4.3)
OID: 1.3.6.1.4.1.25623.1.0.805188

443/tcp (https)

Summary
This host is installed with OpenSSL and is prone to man in the middle attack.

Affected Nodes
192.168.1.201, 192.168.1.202

Vulnerability Detection Result
DHE_EXPORT cipher suites supported by the remote server: TLSv1.0: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0014) TLSv1.1: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0014) TLSv1.2: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0014)

Impact
Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream. Impact Level: Application

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

Vulnerability Insight
Flaw is triggered when handling Diffie-Hellman key exchanges defined in the DHE_EXPORT cipher

Vulnerability Detection Method
Send a crafted 'Client Hello' request and check the servers response. Details: OpenSSL TLS 'DHE_EXPORT' LogJam Man in the Middle Security Bypass Vulnerabil... (OID: 1.3.6.1.4.1.25623.1.0.805188) Version used: $Revision: 4098 $

References

https://weakdh.org, https://weakdh.org/imperfect-forward-secrecy.pdf, http://openwall.com/lists/oss-security/2015/05/20/8, https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained, https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes

2.97 - PHP Cross-Site Scripting Vulnerability - Aug16 (Linux)

Medium: (CVSS: 4.3)
OID: 1.3.6.1.4.1.25623.1.0.809137
80/tcp (http)

Summary
This host is installed with PHP and is prone to cross-site scripting (XSS) vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.4.38

Impact
Successfully exploiting this issue allows remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer by leveraging '%0A%20' or '%0D%0A%20' mishandling in the header function. Impact Level: Application

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

Vulnerability Insight
The flaw is due to the 'sapi_header_op' function in 'main/SAPI.c' script supports deprecated line folding without considering browser compatibility.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Cross-Site Scripting Vulnerability - Aug16 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.809137) Version used: $Revision: 4161 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
https://bugs.php.net/bug.php?id=68978

2.98 - PHP LibGD Denial of Service Vulnerability

Medium: (CVSS: 4.3)
OID: 1.3.6.1.4.1.25623.1.0.804292
80/tcp (http)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.4.32/5.5.16/5.6.0

Impact
Successful exploitation will allow remote attackers to conduct denial of service attacks. Impact Level: Application

Solution
Upgrade to PHP version 5.4.32 or 5.5.16 or 5.6.0 or later. For updates refer to http://php.net

Vulnerability Insight
The flaw is due to a NULL pointer dereference error in 'gdImageCreateFromXpm' function within LibGD.

Vulnerability Detection Method

Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not. Details: PHP 'LibGD' Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.804292) Version used: $Revision: 3942 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
https://bugs.php.net/bug.php?id=66901

2.99 - OpenSSH Security Bypass Vulnerability

M **Medium**: (CVSS: 4.3)
OID: 1.3.6.1.4.1.25623.1.0.806049 — 22/tcp (ssh)

Summary
This host is running OpenSSH and is prone to security bypass vulnerability.

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)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: 6.9
Multiple results by host

Impact
Successful exploitation will allow remote attackers to bypass intended access restrictions. Impact Level: Application

Solution
Upgrade to OpenSSH version 6.9 or later. For updates refer to http://www.openssh.com

Vulnerability Insight
The flaw is due to the refusal deadline was not checked within the x11_open_helper function.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: OpenSSH Security Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.806049) Version used: $Revision: 2676 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.3 Method: SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

References
http://openwall.com/lists/oss-security/2015/07/01/10

2.100 - POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

M **Medium**: (CVSS: 4.3)
OID: 1.3.6.1.4.1.25623.1.0.802087 — 443/tcp (https)

Summary
This host is prone to an information disclosure vulnerability.

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)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream. Impact Level: Application

Solution
Disable SSL v3.0

Vulnerability Insight
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method
Send a SSLv3 request and check the response. Details: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802087) Version used: $Revision: 4161 $

References
https://www.openssl.org/~bodo/ssl-poodle.pdf, https://www.imperialviolet.org/2014/10/14/poodle.html, https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html, http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

2.101 - PHP SOAP Parser Multiple Information Disclosure Vulnerabilities

M **Medium**: (CVSS: 4.3) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.803764

Summary
This host is installed with PHP and is prone to multiple information disclosure vulnerabilities.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.3.22/5.4.12

Impact
Successful exploitation will allow remote attackers to obtain sensitive information. Impact Level: Application

Solution
Upgrade to PHP 5.3.22 or 5.4.12 or later, http://www.php.net/downloads.php

Vulnerability Insight
Flaws are due to the way SOAP parser process certain SOAP objects (due to allowed expansion of XML external entities during SOAP WSDL files parsing).

Vulnerability Detection Method
Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not. Details: PHP SOAP Parser Multiple Information Disclosure Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.803764) Version used: $Revision: 3942 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://php.net/ChangeLog-5.php, http://git.php.net/?p=php-src.git;a=commit;h=afe98b7829d50806559acac9b530acb8283c3bf4

2.102 - Deprecated SSLv2 and SSLv3 Protocol Detection

M **Medium**: (CVSS: 4.3) 443/tcp (https)
OID: 1.3.6.1.4.1.25623.1.0.111012

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

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)

Vulnerability Detection Result
In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'Check SSL Weak Ciphers and Supported Ciphers' NVT. Multiple results by host

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

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.

Vulnerability Insight
The SSLv2 and SSLv3 protocols containing known cryptographic flaws.

Vulnerability Detection Method
Check the used protocols of the services provided by this system. Details: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012) Version used: $Revision: 4007 $

References
https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, https://bettercrypto.org/

2.103 - ISC BIND AXFR Response Denial of Service Vulnerability

M **Medium**: (CVSS: 4) 53/tcp (domain)
OID: 1.3.6.1.4.1.25623.1.0.106118

Summary
ISC BIND is prone to a denial of service vulnerability.

Affected Nodes
192.168.3.2

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An authenticated remote attacker may cause a denial of service condition.

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.

Vulnerability Insight
Primary DNS servers may cause a denial of service (secondary DNS server crash) via a large AXFR response, and possibly allows IXFR servers to cause a denial of service (IXFR client crash) via a large IXFR response and allows remote authenticated accts to cause a denial of service (primary DNS server crash) via a large UPDATE message

Vulnerability Detection Method
Checks the version. Details: ISC BIND AXFR Response Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.106118) Version used: $Revision: 4087 $

Product Detection Result
Product: cpe:/a:isc:bind:1.5.9 Method: Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)

References
http://www.openwall.com/lists/oss-security/2016/07/06/3, https://lists.dns-oarc.net/pipermail/dns-operations/2016-July/015058.html

2.104 - SSL Certificate Signed Using A Weak Signature Algorithm

Medium: (CVSS: 4)
OID: 1.3.6.1.4.1.25623.1.0.105880
443/tcp (https)

Summary
The remote service is using a SSL certificate chain that has been signed using a cryptographically weak hashing algorithm.

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)

Vulnerability Detection Result
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: CN=Ruckus Wireless Inc. SN-251204007096,O=Ruckus Wireless Inc,L=Sunnyvale,ST=California,C=US Signature Algorithm: sha1WithRSAEncryption Subject: O=Ruckus Wireless\, Inc.,L=Sunnyvale,ST=California,C=US Signature Algorithm: sha1WithRSAEncryption
Multiple results by host

Vulnerability Insight
Secure Hash Algorithm 1 (SHA-1) is considered cryptographically weak and not secure enough for ongoing use. Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning accts when accts visit web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates. Servers that use SSL certificates signed using an SHA-1 signature will need to obtain new SHA-2 signed SSL certificates to avoid these web browser SSL certificate warnings.

Vulnerability Detection Method
Check which algorithm was used to sign the remote SSL Certificate. Details: SSL Certificate Signed Using A Weak Signature Algorithm (OID: 1.3.6.1.4.1.25623.1.0.105880) Version used: $Revision: 4061 $

References
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

2.105 - SSL Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Medium: (CVSS: 4)
OID: 1.3.6.1.4.1.25623.1.0.106223
443/tcp (https)

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

Affected Nodes
192.168.1.1, 192.168.1.203, 192.168.1.205, 192.168.5.1, 192.168.6.49

Vulnerability Detection Result
Server Temporary Key Size: 1024 bits

Impact

An attacker might be able to decrypt the TLS communication offline.

Solution
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see https://weakdh.org/sysadmin.html)

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size. Details: SSL Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.106223) Version used: $Revision: 3974 $

References
https://weakdh.org/

2.106 - Samba Overwrite ACLs Vulnerability

M	**Medium**: (CVSS: 4) **OID:** 1.3.6.1.4.1.25623.1.0.807711	445/tcp (microsoft-ds)

Summary
This host is running Samba and is prone to overwrite ACLs vulnerability.

Affected Nodes
192.168.1.50(myco-bdr), 192.168.6.82(MINTLINUX)

Vulnerability Detection Result
Installed version: 3.6.3 Fixed version: 4.1.23
Multiple results by host

Impact
Successful exploitation will allow a remote attacker to gain access to an arbitrary file or directory by overwriting its ACL. Impact Level: Application

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

Vulnerability Insight
The flaw exist due to an improper handling of the request,a UNIX SMB1 call, to create a symlink.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: Samba Overwrite ACLs Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.807711) Version used: $Revision: 3000 $

Product Detection Result
Product: cpe:/a:samba:samba:3.6.3 Method: SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

References
https://www.samba.org/samba/security/CVE-2015-7560.html

2.107 - openssh-server Forced dbre Handling Information Disclosure Vulnerability

L	**Low**: (CVSS: 3.5) **OID:** 1.3.6.1.4.1.25623.1.0.103503	22/tcp (ssh)

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 directory.

Affected Nodes
192.168.0.3, 192.168.1.203, 192.168.1.204, 192.168.1.205

Vulnerability Detection Result
According to its banner, the version of OpenSSH installed on the remote host is older than 5.7: SSH-1.99-OpenSSH_4.3
Multiple results by host

Solution
Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details: openssh-server Forced dbre Handling Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103503) Version used: $Revision: 3445 $

References
http://www.securityfocus.com/bid/51702, http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445, http://packages.debian.org/squeeze/openssh-server, https://downloads.avaya.com/css/P8/documents/100161262

2.108 - OpenSSH ssh_gssapi_parse_ename() Function Denial of Service Vulnerability

L	**Low**: (CVSS: 3.5) **OID:** 1.3.6.1.4.1.25623.1.0.103937	22/tcp (ssh)

Summary
OpenSSH is prone to a remote denial-of-service vulnerability.

Affected Nodes
192.168.0.3, 192.168.1.203, 192.168.1.204, 192.168.1.205

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Exploiting this issue allows remote attackers to trigger denial-of-service conditions due to excessive memory consumption.

Solution
Updates are available. Please see the references for details.

Vulnerability Detection Method
Check the version. Details: OpenSSH 'ssh_gssapi_parse_ename()' Function Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103937) Version used: $Revision: 3445 $

References
http://www.securityfocus.com/bid/54114, http://www.openssh.com

2.109 - SSH Weak MAC Algorithms Supported

L	**Low**: (CVSS: 2.6) **OID:** 1.3.6.1.4.1.25623.1.0.105610	22/tcp (ssh)

Summary
The remote SSH server is configured to allow weak MD5 and/or 96-bit 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

Vulnerability Detection Result

The following weak client-to-server MAC algorithms are supported by the remote service: hmac-md5 hmac-sha1-96 hmac-md5-96 The following weak server-to-client MAC algorithms are supported by the remote service: hmac-md5 hmac-sha1-96 hmac-md5-96
Multiple results by host

Solution
Disable the weak MAC algorithms.

Vulnerability Detection Method
Details: SSH Weak MAC Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105610) Version used: $Revision: 3157 $

2.110 - OpenSSH CBC Mode Information Disclosure Vulnerability

L	**Low**: (CVSS: 2.6) **OID:** 1.3.6.1.4.1.25623.1.0.100153	22/tcp (ssh)

Summary
The host is installed with OpenSSH and is prone to information disclosure vulnerability.

Affected Nodes
192.168.0.3, 192.168.1.205

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploits will allow attackers to obtain four bytes of plaintext from an encrypted session. Impact Level: Application

Solution
Upgrade to higher version http://www.openssh.com/portable.html

Vulnerability Insight
The flaw is due to the improper handling of errors within an SSH session encrypted with a block cipher algorithm in the Cipher-Block Chaining 'CBC' mode.

Vulnerability Detection Method
Details: OpenSSH CBC Mode Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.100153) Version used: $Revision: 3445 $

References
http://www.securityfocus.com/bid/32319

2.111 - Relative IP Identification number change

L	**Low**: (CVSS: 2.6) **OID:** 1.3.6.1.4.1.25623.1.0.10201	

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.

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

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An attacker may use this feature to determine traffic patterns within your redi. A few examples (not at all exhaustive) are: 1. A remote attacker can determine if the remote host sent a packet in reply to another request. Specifically, an attacker can use your server as an unwilling participant in a blind portscan of another redi. 2. A remote attacker can roughly determine server requests at certain times of the day. For instance, if the server is

sending much more traffic after business hours, the server may be a reverse proxy or other remote access device. An attacker can use this information to concentrate his/her efforts on the more critical machines. 3. A remote attacker can roughly estimate the number of requests that a web server processes over a period of time.

Solution
Contact your vendor for a patch

Vulnerability Detection Method
Details: Relative IP Identification number change (OID: 1.3.6.1.4.1.25623.1.0.10201) Version used: $Revision: 4048 $

2.112 - TCP timestamps

Low: (CVSS: 2.6)
OID: 1.3.6.1.4.1.25623.1.0.80091

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

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), 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)

Vulnerability Detection Result
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 20309330 Paket 2: 20309332
Multiple results by host

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

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

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091) Version used: $Revision: 4048 $

References
http://www.ietf.org/rfc/rfc1323.txt

2.113 - PHP Information Disclosure Vulnerability - 01 - Sep14

L	**Low**: (CVSS: 2.6) **OID:** 1.3.6.1.4.1.25623.1.0.804849	80/tcp (http)

Summary
This host is installed with PHP and is prone to information disclosure vulnerability.

Affected Nodes
192.168.1.50(myco-bdr)

Vulnerability Detection Result
Installed version: 5.3.10 Fixed version: 5.3.29/5.4.30/5.5.14

Impact
Successful exploitation will allow a local attacker to gain access to sensitive information. Impact Level: Application

Solution
Upgrade to PHP version 5.3.29 or 5.4.30 or 5.5.14 or later

Vulnerability Insight
The flaw is due to an error in the 'hp_print_info' function within /ext/standard/info.c script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: PHP Information Disclosure Vulnerability - 01 - Sep14 (OID: 1.3.6.1.4.1.25623.1.0.804849) Version used: $Revision: 3942 $

Product Detection Result
Product: cpe:/a:php:php:5.3.10 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References
http://php.net/ChangeLog-5.php, https://bugs.php.net/bug.php?id=67498, https://www.sektioneins.de/en/blog/14-07-04-phpinfo-infoleak.html

2.114 - OpenSSH ssh-codesign.c Local Information Disclosure Vulnerability

L	**Low**: (CVSS: 2.1) **OID:** 1.3.6.1.4.1.25623.1.0.105002	22/tcp (ssh)

Summary
OpenSSH is prone to a local information-disclosure vulnerability.

Affected Nodes
192.168.0.3, 192.168.1.203, 192.168.1.204, 192.168.1.205

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Local attackers can exploit this issue to obtain sensitive information. Information obtained may lead to further attacks.

Solution
Updates are available.

Vulnerability Insight
ssh-codesign.c in ssh-codesign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local accts to obtain sensitive key information via the ptrace system call.

Vulnerability Detection Method
Check the version. Details: OpenSSH 'ssh-codesign.c' Local Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.105002) Version used: $Revision: 3445 $

References
http://www.securityfocus.com/bid/65674, http://www.openssh.com, http://www.openssh.com/txt/portable-codesign-rand-helper.adv