YourIT!
Your Logo Goes Here

PCI Assessment

Internal Vulnerability Scan Detail by Issue Report

Scan Date: 5/7/2015

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

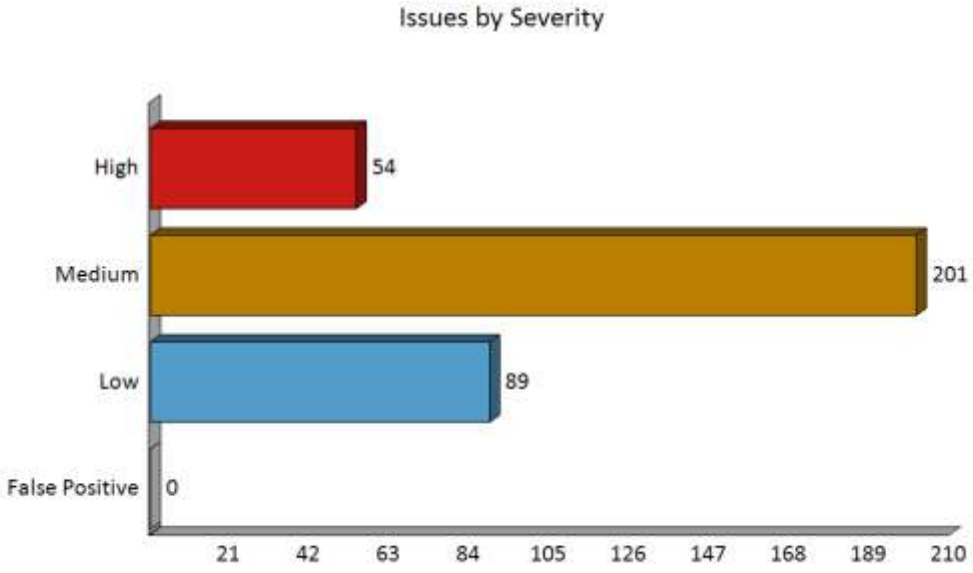
5/11/2015

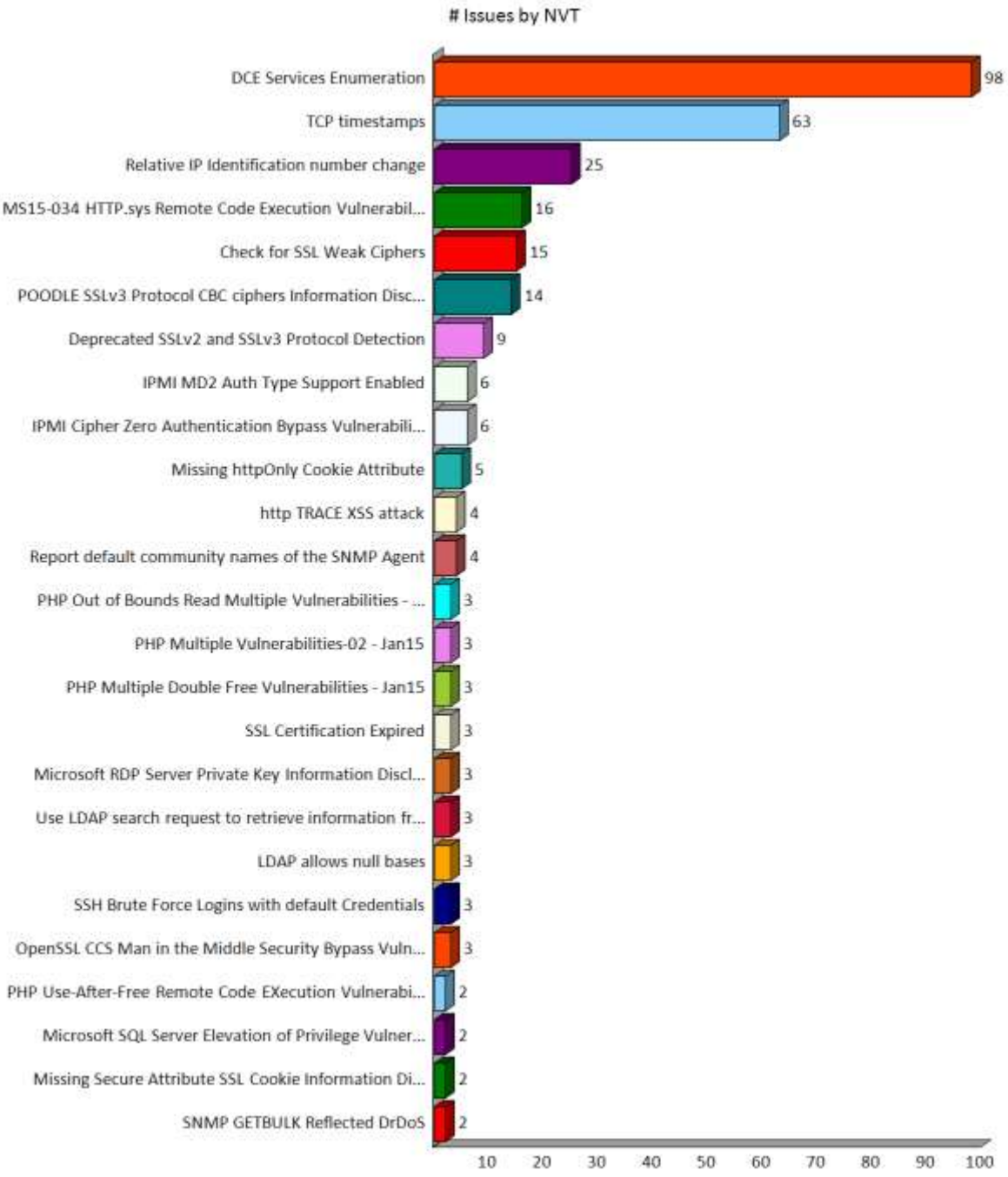
Table of Contents

2.47 - PHP CDF File Parsing Denial of Service Vulnerabilities -01 Jun14
2.48 - PHP SSL Certificate Validation Security Bypass Vulnerability (Windows)
2.49 - PHP SOAP Parser Multiple Information Disclosure Vulnerabilities
2.50 - PHP LibGD Denial of Service Vulnerability
2.51 - Apache HTTP Server httpOnly Cookie Information Disclosure Vulnerability
2.52 - PHP Information Disclosure Vulnerability-01 Sep14
2.53 - Microsoft IIS FTPd NLST stack overflow
2.54 - Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387)
2.55 - Windows Administrator NULL FTP password
2.56 - Apache Tomcat servlet/JSP container default files
2.57 - Apache Tomcat Multiple Vulnerabilities - 01 Mar14
2.58 - IIS Service Pack - 404
2.59 - Microsoft ASP.NET Information Disclosure Vulnerability (2418042)
2.60 - Microsoft IIS IP Address/Internal Network Name Disclosure Vulnerability
2.61 - Apache Tomcat Multiple Vulnerabilities June-09
2.62 - Apache Tomcat Cross-Site Scripting and Security Bypass Vulnerabilities
2.63 - Microsoft IIS Default Welcome Page Information Disclosure Vulnerability
2.64 - Apache Tomcat JSP Example Web Applications Cross Site Scripting Vulnerability
2.65 - Apache Tomcat RemoteFilterValve Security Bypass Vulnerability
2.66 - Apache Tomcat Multiple Vulnerabilities - 02 Mar14
2.67 - Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)
2.68 - Microsoft Windows SMTP Server DNS spoofing vulnerability
2.69 - Microsoft Windows SMTP Server MX Record Denial of Service Vulnerability

1 - Summary

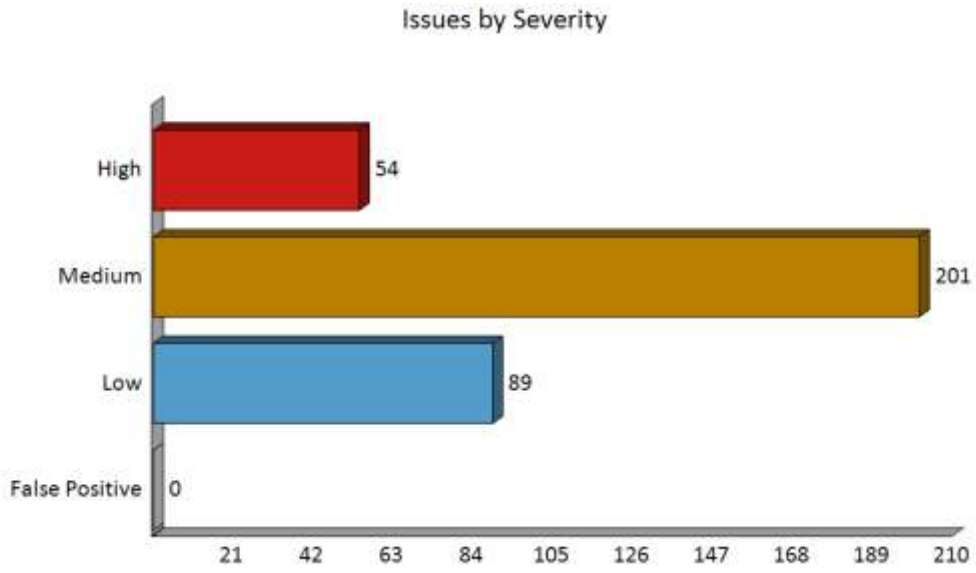
This report gives details on hosts that were tested and issues that were found group by individual issues.




Issues by NVT
DCE Services Enumeration 98
TCP timestamps 63
Relative IP Identification number change 25
MS15-034 HTTP.sys Remote Code Execution Vulnerabil... 16
Check for SSL Weak Ciphers 15
POODLE SSLv3 Protocol CBC ciphers Information Disc... 14
Deprecated SSLv2 and SSLv3 Protocol Detection 9
IPMI MD2 Auth Type Support Enabled 6
IPMI Cipher Zero Authentication Bypass Vulnerabili... 6
Missing httpOnly Cookie Attribute 5
http TRACE XSS attack 4
Report default community names of the SNMP Agent 4
PHP Out of Bounds Read Multiple Vulnerabilities - ... 3
PHP Multiple Vulnerabilities-02 - Jan15 3
PHP Multiple Double Free Vulnerabilities - Jan15 3
SSL Certification Expired 3
Microsoft RDP Server Private Key Information Discl... 3
Use LDAP search request to retrieve information fr... 3
LDAP allows null bases 3
SSH Brute Force Logins with default Credentials 3
OpenSSL CCS Man in the Middle Security Bypass Vuln... 3
PHP Use-After-Free Remote Code EXecution Vulnerabi... 2
Microsoft SQL Server Elevation of Privilege Vulner... 2
Missing Secure Attribute SSL Cookie Information Di... 2
SNMP GETBULK Reflected DrDoS 2
10 20 30 40 50 60 70 80 90 100

Issues by NVT (continued)

2 - Scan Details



2.1 - Report default community names of the SNMP Agent

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

Summary

Simple Network Management Protocol (SNMP) is a protocol which can be used by administrators to remotely manage a computer or network device. There are typically 2 modes of remote SNMP monitoring. These modes are roughly 'READ' and 'WRITE' (or PUBLIC and PRIVATE).

Affected Nodes

10.0.0.1, 10.0.0.11, 10.0.0.21, 10.0.1.51

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 network 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: 1108 $

2.2 - OpenSSL CCS Man in the Middle Security Bypass Vulnerability

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

10.0.0.1, 10.0.1.240, 10.0.6.49

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: 1153 $

References

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

2.3 - SNMP GETBULK Reflected DrDoS

Medium (CVSS: 5) 161/udp (snmp)
OID: 1.3.6.1.4.1.25623.1.0.105062

Summary

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

Affected Nodes

10.0.0.1, 10.0.1.52

Vulnerability Detection Result

By sending a SNMP GetBulk request of 41 bytes, we received a response of 1268 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: 1108 $

References

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

2.4 - POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

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

Summary

This host is installed with OpenSSL and is prone to information disclosure vulnerability.

Affected Nodes

10.0.0.1, 10.0.1.1, 10.0.1.5(VPNGW), 10.0.1.15(UTIL12), 10.0.1.21(RDGATEWAY), 10.0.1.69(STORAGE01), 10.0.1.81(FINANCE), 10.0.1.202, 10.0.1.240, 10.0.5.1, 10.0.6.49, 10.0.6.50(SVRDEV2), 10.0.6.103(USER-HP), 10.0.6.107(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

Vendor released a patch to address this vulnerabiliy, For updates contact vendor or refer to https://www.openssl.org NOTE: The only correct way to fix POODLE is to disable SSL v3.0

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: 1152 $

References

http://osvdb.com/113251, 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

2.5 - 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

10.0.0.1, 10.0.0.11, 10.0.0.21, 10.0.1.3(DC03), 10.0.1.4, 10.0.1.5(VPNGW), 10.0.1.15(UTIL12), 10.0.1.16(DEVTFS), 10.0.1.21(RDGATEWAY), 10.0.1.23, 10.0.1.41(FILE2012-1), 10.0.1.50(MYCO-DATTO), 10.0.1.51, 10.0.1.52, 10.0.1.69(STORAGE01), 10.0.1.81(FINANCE), 10.0.1.100(HV00), 10.0.1.104(HV04), 10.0.1.120(HV02), 10.0.1.121(HV02), 10.0.1.201, 10.0.1.202, 10.0.1.203, 10.0.1.204, 10.0.1.205, 10.0.1.240, 10.0.3.2, 10.0.6.0(MWEST-PC), 10.0.6.1(REX), 10.0.6.4(CCSVR01), 10.0.6.12(SVRTEST1), 10.0.6.14, 10.0.6.20(SVRDEV3), 10.0.6.33(CONFERENCEROOM), 10.0.6.35(BROWND), 10.0.6.40(PSIMPSON-PC), 10.0.6.41(QA-PC), 10.0.6.44(JIM-WIN7), 10.0.6.47(PKWIN8), 10.0.6.49, 10.0.6.50(SVRDEV2), 10.0.6.53(PSIMPSON-WIN7TEST), 10.0.6.55(CONFERENCEROOM), 10.0.6.67(DEVTFSBUILD), 10.0.6.76(SVRDEMO1), 10.0.6.80(PS01), 10.0.6.86(SVRRFT1), 10.0.6.88(JRAWIN8K1QA3), 10.0.6.96(MWEST-WIN864), 10.0.6.97(RANCOR), 10.0.6.103(USER-HP), 10.0.6.106(PABLO-HOME), 10.0.6.107(VPNGW), 10.0.6.109(SVRTEST2), 10.0.6.122, 10.0.6.133(WRKMARCUS-PC), 10.0.7.18(PSIMPSON-WIN764), 10.0.7.44(JIM-WIN8), 10.0.7.45(TDDESKTOP-DT), 10.0.7.74(BKRICKEY-WIN81), 10.0.7.89, 10.0.7.95(MMAYHEMON-HP), 10.0.7.123(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: 2008676 Paket 2: 2008679

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: 787 $

References

http://www.ietf.org/rfc/rfc1323.txt

2.6 - Web Server Cross Site Scripting

Medium (CVSS: 4.3) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.10815

Summary

The remote web server seems to be vulnerable to a Cross Site Scripting vulnerability (XSS). The vulnerability is caused by the result being returned to the user when a non-existing file is requested (e.g. the result contains script code provided in the request). This vulnerability would allow an attacker to make the server present the user with the attacker's JavaScript/HTML code. Since the content is presented by the server, the user will give it the trust level of the server (for example, the websites banks, shopping centers, etc. would usually be trusted by a user). Solutions: . Allaire/Macromedia Jrun: - http://www.macromedia.com/software/jrun/download/update/ [^] - http://www.securiteam.com/windowsntfocus/Allaire_fixes_Cross-Site_Scripting_security_vulnerability.html [^] . Microsoft IIS: - http://www.securiteam.com/windowsntfocus/IIS_Cross-Site_scripting_vulnerability__Patch_available_.html [^] . Apache: - http://httpd.apache.org/info/css-security/ [^] . Bluecoat CacheOS: - http://download.cacheflow.com/release/CA/4.1.00-docs/CACacheOS41fixes.htm [^] . ColdFusion: - http://www.macromedia.com/v1/handlers/index.cfm?ID=23047 [^] . General: - http://www.securiteam.com/exploits/Security_concerns_when_developing_a_dynamically_generated_web_site.html [^] - http://www.cert.org/advisories/CA-2000-02.html [^]

Affected Nodes

10.0.0.11

Vulnerability Detection Result

The remote web server seems to be vulnerable to the Cross Site Scripting vulnerability (XSS). The vulnerability is caused by the result returned to the user when a non-existing file is requested (e.g. the result contains the JavaScript provided in the request). The vulnerability would allow an attacker to make the server present the user with the attacker's JavaScript/HTML code. Since the content is presented by the server, the user will give it the trust level of the server (for example, the trust level of banks, shopping centers, etc. would usually be high). Sample url : http://10.0.0.11:80/<SCRIPT>foo</SCRIPT> Solutions: . Allaire/Macromedia Jrun: - http://www.macromedia.com/software/jrun/download/update/ - http://www.securiteam.com/windowsntfocus/Allaire_fixes_Cross-Site_Scripting_security_vulnerability.html . Microsoft IIS: - http://www.securiteam.com/windowsntfocus/IIS_Cross-Site_scripting_vulnerability__Patch_available_.html . Apache: - http://httpd.apache.org/info/css-security/ . ColdFusion: - http://www.macromedia.com/v1/handlers/index.cfm?ID=23047 . General: - http://www.securiteam.com/exploits/Security_concerns_when_developing_a_dynamically_generated_web_site.html - http://www.cert.org/advisories/CA-2000-02.html

Vulnerability Detection Method

Details: Web Server Cross Site Scripting (OID: 1.3.6.1.4.1.25623.1.0.10815) Version used: $Revision: 41 $

2.7 - Multiple NetGear ProSafe Switches Information Disclosure Vulnerability

High (CVSS: 7.8)	80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.103773	

Summary

Multiple NetGear ProSafe switches are prone to an information- disclosure vulnerability.

Affected Nodes

10.0.0.21

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

An attacker can exploit this issue to download configuration file and disclose sensitive information. Information obtained may aid in further attacks. Impact Level: Application

Solution

Ask the Vendor for an update.

Vulnerability Insight

The web management application fails to restrict URL access to differenti application areas. Remote, unauthenticated attackers could exploit this issue to download the device's startup-config, which contains administrator credentials in encrypted form.

Vulnerability Detection Method

Try to read /filesystem/startup-config with a HTTP GET request and check the response. Details: Multiple NetGear ProSafe Switches Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103773) Version used: $Revision: 155 $

References

http://www.securityfocus.com/bid/61918, http://www.netgear.com

2.8 - SSH Brute Force Logins with default Credentials

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

Summary

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

Affected Nodes

10.0.1.1, 10.0.5.1, 10.0.6.122

Vulnerability Detection Result

It was possible to login with the following credentials <User>:<Password> admin:password

Multiple results by host

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: 1188 $

2.9 - Missing Secure Attribute SSL Cookie Information Disclosure Vulnerability

Medium (CVSS: 6.4) 443/tcp (https)
OID: 1.3.6.1.4.1.25623.1.0.902661

Summary

The host is running a server with SSL and is prone to information disclosure vulnerability.

Affected Nodes

10.0.1.1, 10.0.5.1

Vulnerability Detection Result

The cookies: Set-Cookie: session=; path=/; are missing the secure attribute.

Vulnerability Insight

The flaw is due to SSL cookie is not using 'secure' attribute, which allows cookie to be passed to the server by the client over non-secure channels (http) and allows attacker to conduct session hijacking attacks. remote systems. Impact Level: Application

Vulnerability Detection Method

Details: Missing Secure Attribute SSL Cookie Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902661) Version used: $Revision: 836 $

References

http://www.ietf.org/rfc/rfc2965.txt, https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)

2.10 - Missing httpOnly Cookie Attribute

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

Summary

The application is missing the 'httpOnly' cookie attribute

Affected Nodes

10.0.1.1, 10.0.5.1, 10.0.7.65(MYCO30DEV)

Vulnerability Detection Result

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

Multiple results by host

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: 809 $

References

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

2.11 - Relative IP Identification number change

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. An attacker may use this feature to determine traffic patterns within your network. 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 network. 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.

Affected Nodes

10.0.1.1, 10.0.1.6(ISA1), 10.0.1.15(UTIL12), 10.0.1.51, 10.0.1.52, 10.0.1.81(FINANCE), 10.0.3.204, 10.0.5.1, 10.0.6.0(MWEST-PC), 10.0.6.1(REX), 10.0.6.4(CCSVR01), 10.0.6.33(CONFERENCEROOM), 10.0.6.35(BROWND), 10.0.6.41(QA-PC), 10.0.6.44(JIM-WIN7), 10.0.6.47(PKWIN8), 10.0.6.55(CONFERENCEROOM), 10.0.6.67(DEVTFSBUILD), 10.0.6.69(ISA1), 10.0.6.107(VPNGW), 10.0.6.133(WRKMARCUS-PC), 10.0.7.18(PSIMPSON-WIN764), 10.0.7.74(BKRICKEY-WIN81), 10.0.7.95(MMAYHEMON-HP), 10.0.7.123(ISTCORP-PC)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

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: 1048 $

2.12 - DCE Services Enumeration

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

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

10.0.1.3(DC03), 10.0.1.4, 10.0.1.5(VPNGW), 10.0.1.6(ISA1), 10.0.1.15(UTIL12), 10.0.1.16(DEVTFS), 10.0.1.21(RDGATEWAY), 10.0.1.23, 10.0.1.41(FILE2012-1), 10.0.1.69(STORAGE01), 10.0.1.81(FINANCE), 10.0.1.100(HV00), 10.0.1.104(HV04), 10.0.1.120(HV02), 10.0.1.121(HV02), 10.0.6.0(MWEST-PC), 10.0.6.1(REX), 10.0.6.4(CCSVR01), 10.0.6.12(SVRTEST1), 10.0.6.14, 10.0.6.20(SVRDEV3), 10.0.6.33(CONFERENCEROOM), 10.0.6.35(BROWND), 10.0.6.40(PSIMPSON-PC), 10.0.6.41(QA-PC), 10.0.6.44(JIM-WIN7), 10.0.6.47(PKWIN8), 10.0.6.53(PSIMPSON-WIN7TEST), 10.0.6.55(CONFERENCEROOM), 10.0.6.67(DEVTFSBUILD), 10.0.6.69(ISA1), 10.0.6.76(SVRDEMO1), 10.0.6.80(PS01), 10.0.6.86(SVRRFT1), 10.0.6.88(JRAWIN8K1QA3), 10.0.6.96(MWEST-WIN864), 10.0.6.97(RANCOR), 10.0.6.103(USER-HP), 10.0.6.106(PABLO-HOME), 10.0.6.107(VPNGW), 10.0.6.109(SVRTEST2), 10.0.6.133(WRKMARCUS-PC), 10.0.7.18(PSIMPSON-WIN764), 10.0.7.44(JIM-WIN8), 10.0.7.45(TDDESKTOP-DT), 10.0.7.65(MYCO30DEV), 10.0.7.74(BKRICKEY-WIN81), 10.0.7.95(MMAYHEMON-HP), 10.0.7.123(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: 41 $

2.13 - LDAP allows null bases

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

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 user can query your LDAP server using a tool such as 'LdapMiner'

Affected Nodes

10.0.1.3(DC03), 10.0.1.4, 10.0.1.23

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: 966 $

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

Medium (CVSS: 5) 389/tcp (ldap)
OID: 1.3.6.1.4.1.25623.1.0.12105

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

10.0.1.3(DC03), 10.0.1.4, 10.0.1.23

Vulnerability Detection Result

Summary: It is possible to disclose LDAP information. Description : The directory base of the remote server is set to NULL. This allows information to be enumerated without any prior knowledge of the directory structure. Solution: If pre-Windows 2000 compatibility is not required, remove pre-Windows 2000 compatibility as follows : - start cmd.exe - execute the command : net localgroup 'Pre-Windows 2000 Compatible Access' everyone /delete - restart the remote host Plugin output : 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 command : 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: 128 $

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

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

10.0.1.5(VPNGW), 10.0.1.15(UTIL12), 10.0.1.21(RDGATEWAY), 10.0.1.69(STORAGE01), 10.0.1.81(FINANCE), 10.0.6.12(SVRTEST1), 10.0.6.20(SVRDEV3), 10.0.6.50(SVRDEV2), 10.0.6.76(SVRDEMO1), 10.0.6.86(SVRRFT1), 10.0.6.107(VPNGW), 10.0.6.109(SVRTEST2)

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 user and to perform actions in the security context of the current user.

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: 1177 $

Product Detection Result

Product: cpe:/a:microsoft:iis:8.5 Method: Microsoft IIS Webserver Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900710)

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

2.16 - Check for SSL Weak Ciphers

Medium (CVSS: 4.3) 443/tcp (https)
OID: 1.3.6.1.4.1.25623.1.0.103440

Summary

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

Affected Nodes

10.0.1.5(VPNGW), 10.0.1.15(UTIL12), 10.0.1.21(RDGATEWAY), 10.0.1.69(STORAGE01), 10.0.1.81(FINANCE), 10.0.1.201, 10.0.1.202, 10.0.1.203, 10.0.1.204, 10.0.1.205, 10.0.1.240, 10.0.6.49, 10.0.6.50(SVRDEV2), 10.0.6.107(VPNGW), 10.0.6.122

Vulnerability Detection Result

Weak ciphers offered by this service: SSL3_RSA_RC4_128_MD5 SSL3_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_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. - 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: 733 $

2.17 - Deprecated SSLv2 and SSLv3 Protocol Detection

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

10.0.1.5(VPNGW), 10.0.1.15(UTIL12), 10.0.1.21(RDGATEWAY), 10.0.1.69(STORAGE01), 10.0.1.81(FINANCE), 10.0.1.240, 10.0.6.49, 10.0.6.50(SVRDEV2), 10.0.6.107(VPNGW)

Vulnerability Detection Result

In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers.

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 transfered 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: 1183 $

References

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

2.18 - Microsoft RDP Server Private Key Information Disclosure Vulnerability

Medium (CVSS: 6.4) 3389/tcp
OID: 1.3.6.1.4.1.25623.1.0.902658

Summary

This host is running Remote Desktop Protocol server and is prone to information disclosure vulnerability.

Affected Nodes

10.0.1.6(ISA1), 10.0.6.69(ISA1), 10.0.7.65(MYCO30DEV)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation could allow remote attackers to gain sensitive information. Impact Level: System/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. A Workaround is to connect only to terminal services over trusted networks.

Vulnerability Insight

The flaw is due to RDP server which stores an RSA private key used for signing a terminal server's public key in the mstlsapi.dll library, which allows remote attackers to calculate a valid signature and further perform a man-in-the-middle (MITM) attacks to obtain sensitive information.

Vulnerability Detection Method

Details: Microsoft RDP Server Private Key Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902658) Version used: $Revision: 666 $

References

http://secunia.com/advisories/15605/, http://xforce.iss.net/xforce/xfdb/21954, http://www.oxid.it/downloads/rdp-gbu.pdf, http://sourceforge.net/p/xrdp/mailman/message/32732056

2.19 - SSL Certification Expired

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

Summary

The remote server's SSL certificate has already expired.

Affected Nodes

10.0.1.15(UTIL12), 10.0.1.69(STORAGE01), 10.0.1.81(FINANCE)

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: 626 $

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

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

10.0.1.16(DEVTFS), 10.0.6.80(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: 856 $

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

http://osvdb.com/109932, http://osvdb.com/109933, https://technet.microsoft.com/library/security/MS14-044

2.21 - NFS export

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

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

10.0.1.50(MYCO-DATTO)

Vulnerability Detection Result

Here is the export list of 10.0.1.50 : /homePool/10.0.1.69-1423717163-vhd 0.0.0.0/0.0.0.0 /home/MYCO30Dev 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: 43 $

2.22 - X Server

High (CVSS: 10) 6001/tcp (x11-1)
OID: 1.3.6.1.4.1.25623.1.0.10407

Summary

This plugin detects X Window servers. X11 is a client - server protocol. Basically, the server is in charge of the screen, and the clients connect to it and send several requests like drawing a window or a menu, and the server sends events back to the clients, such as mouse clicks, key strokes, and so on... An improperly configured X server will accept connections from clients from anywhere. This allows an attacker to make a client connect to the X server to record the keystrokes of the user, which may contain sensitive information, such as account passwords. This can be prevented by using xauth, MIT cookies, or preventing the X server from listening on TCP (a Unix sock is used for local connections)

Affected Nodes

10.0.1.50(MYCO-DATTO)

Vulnerability Detection Result

This X server does *not* allow any client to connect to it however it is recommended that you filter incoming connections to this port as attacker may send garbage data and slow down your X session or even kill the server. Here is the server version : 11.0 Here is the message we received : Client is not authorized Solution: filter incoming connections to ports 6000-6009

Vulnerability Detection Method

Details: X Server (OID: 1.3.6.1.4.1.25623.1.0.10407) Version used: $Revision: 41 $

2.23 - IPMI Cipher Zero Authentication Bypass Vulnerability

High (CVSS: 10) 623/tcp
OID: 1.3.6.1.4.1.25623.1.0.103840

Summary

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

Affected Nodes

10.0.1.201, 10.0.1.202, 10.0.1.203, 10.0.1.204, 10.0.1.205, 10.0.6.122

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: 83 $

References

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

2.24 - IPMI MD2 Auth Type Support Enabled

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

Summary

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

Affected Nodes

10.0.1.201, 10.0.1.202, 10.0.1.203, 10.0.1.204, 10.0.1.205, 10.0.6.122

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: 79 $

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

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

Summary

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

Affected Nodes

10.0.1.202

Vulnerability Detection Result

EXPORT_RSA cipher suites supported by the remote server: SSLv3: TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0008) SSLv3: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0006) SSLv3: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0003) 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)

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 keys 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: 1142 $

References

https://freakattack.com, http://osvdb.org/116794, http://secpod.org/blog/?p=3818, http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html

2.26 - Dell iDRAC6 and iDRAC7 ErrorMsg Parameter Cross Site Scripting Vulnerability

Medium (CVSS: 4.3) 443/tcp (https)
OID: 1.3.6.1.4.1.25623.1.0.103808

Summary

Dell iDRAC6 and iDRAC7 are prone to a cross-site scripting vulnerability because they fails to properly sanitize user-supplied input.

Affected Nodes

10.0.1.205

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may let the attacker steal cookie-based authentication credentials and launch other attacks.

Solution

Firmware updates will be posted to the Dell support page when available. Users should download the appropriate update for the version of iDRAC they have installed: iDRAC6 'monolithic' (rack and towers) - FW version 1.96 targeted release date is Q4CY13. iDRAC7 all models - FW version 1.46.45 target release date is mid/late September 2013.

Vulnerability Insight

Dell iDRAC 6 and Dell iDRAC 7 administrative web interface login page can allow remote attackers to inject arbitrary script via the vulnerable query string parameter ErrorMsg.

Vulnerability Detection Method

Check the firmware version. Details: Dell iDRAC6 and iDRAC7 'ErrorMsg' Parameter Cross Site Scripting Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.103808) Version used: $Revision: 11 $

Product Detection Result

Product: cpe:/h:dell:remote_access_card:6:firmware_1.20:firmware_1.20 Method: Dell Remote Access Controller Detection (OID: 1.3.6.1.4.1.25623.1.0.103680)

References

http://www.securityfocus.com/bid/62598, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-3589, http://www.kb.cert.org/vuls/id/920038

2.27 - Lighttpd Multiple vulnerabilities

High (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.802072

Summary

This host is running Lighttpd and is prone to multiple vulnerabilities

Affected Nodes

10.0.1.240

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to execute arbitrary SQL commands 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 user supplied input passed via the hostname. - mod_evhost and mod_simple_vhost modules not properly sanitizing user 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: 438 $

References

http://osvdb.org/104381, http://osvdb.org/104382, http://seclists.org/oss-sec/2014/q1/561, http://download.lighttpd.net/lighttpd/security/lighttpd_sa_2014_01.txt

2.28 - Dropbear SSH Server Multiple Security Vulnerabilities

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

Summary

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

Affected Nodes

10.0.1.240

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

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

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 user 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: 1168 $

Product Detection Result

Product: cpe:/a:matt_johnston: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

2.29 - Discard port open

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

10.0.6.69(ISA1)

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: 41 $

2.30 - PHP Use-After-Free Remote Code EXecution Vulnerability - Jan15

High (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.805411

Summary

This host is installed with PHP and is prone to use-after-free vulnerability.

Affected Nodes

10.0.6.103(USER-HP)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to execute arbitrary code via a crafted unserialize call. Impact Level: Application

Solution

Upgrade to PHP version 5.4.36 or 5.5.20 or 5.6.4 or later

Vulnerability Insight

The flaw is due to Use-after-free vulnerability in the process_nested_data function in ext/standard/var _unserializer.re 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 Use-After-Free Remote Code EXecution Vulnerability - Jan15 (OID: 1.3.6.1.4.1.25623.1.0.805411) Version used: $Revision: 907 $

References

http://osvdb.org/116020, http://php.net/ChangeLog-5.php, http://secunia.com/advisories/60920, https://bugs.php.net/bug.php?id=68594

2.31 - PHP Multiple Double Free Vulnerabilities - Jan15

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

10.0.6.103(USER-HP), 10.0.7.45(TDDESKTOP-DT)

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 possibly have unspecified other impact.
Impact Level: Application

Solution

Upgrade to PHP version 5.5.21 or 5.6.5 or later

Vulnerability Insight

The flaw is due to Double free error in the zend_ts_hash_graceful_destroy function in zend_ts_hash.c in the Zend Engine 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 Double Free Vulnerabilities - Jan15 (OID: 1.3.6.1.4.1.25623.1.0.805412) Version used: $Revision: 907 $

References

http://osvdb.org/116499, http://securitytracker.com/id/1031479, https://bugs.php.net/bug.php?id=68676

2.32 - PHP Multiple Vulnerabilities-02 - Jan15

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

10.0.6.103(USER-HP), 10.0.7.45(TDDESKTOP-DT)

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 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: 907 $

References

http://osvdb.org/116500, https://bugs.php.net/bug.php?id=68665, http://securitytracker.com/id/1031480

2.33 - PHP Out of Bounds Read Multiple Vulnerabilities - Jan15

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

10.0.6.103(USER-HP), 10.0.7.45(TDDESKTOP-DT)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

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: 907 $

References

http://osvdb.org/show/osvdb/116621, https://bugs.php.net/bug.php?id=68618

2.34 - http TRACE XSS attack

Medium (CVSS: 5.8) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.11213

Summary

Debugging functions are enabled on the remote HTTP server. The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that

servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Affected Nodes

10.0.6.103(USER-HP), 10.0.7.45(TDDESKTOP-DT), 10.0.7.65(MYCO30DEV)

Vulnerability Detection Result

Solution: Add the following lines for each virtual host in your configuration file : RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F] See also http://httpd.apache.org/docs/current/de/mod/core.html#traceenable

Multiple results by host

Solution

Disable these methods.

Vulnerability Detection Method

Details: http TRACE XSS attack (OID: 1.3.6.1.4.1.25623.1.0.11213) Version used: $Revision: 922 $

References

http://www.kb.cert.org/vuls/id/867593

2.35 - IPMI Default Password Vulnerability

High (CVSS: 8.5) 623/udp (asf-rmcp)
OID: 1.3.6.1.4.1.25623.1.0.105923

Summary

It was possible to find default password/username combinations for the IPMI protocoll.

Affected Nodes

10.0.6.122

Vulnerability Detection Result

Found the following default Username/Password combination: root/calvin

Impact

An attacker can log into the IPMI enabled device often with privileged permissions and gain access to the host operating system. Impact Level: System

Solution

Change the default passwords or disable the default accounts if possible. Filter traffic to UDP port 623.

Vulnerability Insight

Many IPMI enabled devices have set default username/password combinations. If these are not changed or disabled if opens up an easy exploitable vulnerability.

Vulnerability Detection Method

Tries to get a RAKP Message 2 (IPMI v2.0) to check the password hash or activate a session (IPMI v1.5). Details: IPMI Default Password Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.105923) Version used: $Revision: 931 $

References

http://packetstormsecurity.com/files/105730/Supermicro-IPMI-Default-Accounts.html

2.36 - PHP _php_stream_scandir() Buffer Overflow Vulnerability (Windows)

High (CVSS: 10) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.803317

Summary

This host is running PHP and is prone to buffer overflow vulnerability.

Affected Nodes

10.0.7.45(TDDESKTOP-DT)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation could allow attackers to execute arbitrary code and failed attempts will likely result in denial-of-service conditions. Impact Level: System/Application

Solution

upgrade to PHP 5.4.5 or 5.3.15 or later For updates refer to http://www.php.net/downloads.php

Vulnerability Insight

Flaw related to overflow in the _php_stream_scandir function in the stream implementation.

Vulnerability Detection Method

Details: PHP '_php_stream_scandir()' Buffer Overflow Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803317) Version used: $Revision: 81 $

References

http://www.php.net/ChangeLog-5.php, http://en.securitylab.ru/nvd/427456.php, http://secunia.com/advisories/cve_reference/CVE-2012-2688

2.37 - PHP Multiple Vulnerabilities -Marcush 2013 (Windows)

High (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.803337

Summary

This host is running PHP and is prone to multiple vulnerabilities.

Affected Nodes

10.0.7.45(TDDESKTOP-DT)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation allows attackers to read arbitrary files and write wsdl files within the context of the affected application. Impact Level: Application

Solution

Upgrade to PHP 5.4.13 or 5.3.23, which will be availabe soon. For updates refer to http://www.php.net/downloads.php

Vulnerability Insight

Multiple flaws are due to, - Does not validate 'soap.wsdl_cache_dir' directive before writing SOAP wsdl cache files to the filesystem. - Allows the use of external entities while parsing SOAP wsdl files, issue in 'soap_xmlParseFile' and 'soap_xmlParseMemory' functions.

Vulnerability Detection Method

Details: PHP Multiple Vulnerabilities -Marcush 2013 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803337) Version used: $Revision: 81 $

References

http://www.php.net/ChangeLog-5.php, http://bugs.php.net/bug.php?id=64360, http://cxsecurity.com/cveshow/CVE-2013-1635, http://cxsecurity.com/cveshow/CVE-2013-1643, http://bugs.gentoo.org/show_bug.cgi?id=459904

2.38 - PHP phar/tar.c Heap Buffer Overflow Vulnerability (Windows)

High (CVSS: 7.5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.803342

Summary

This host is running PHP and is prone to heap buffer overflow vulnerability.

Affected Nodes

10.0.7.45(TDDESKTOP-DT)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation could allow attackers to execute arbitrary code or cause a denial-of-service condition via specially crafted TAR file. Impact Level: System/Application

Solution

Upgrade to PHP 5.4.4 or 5.3.14 or later For updates refer to http://www.php.net/downloads.php

Vulnerability Insight

Flaw related to overflow in phar_parse_tarfile() function in ext/phar/tar.c in the phar extension.

Vulnerability Detection Method

Details: PHP 'phar/tar.c' Heap Buffer Overflow Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803342) Version used: $Revision: 81 $

References

http://osvdb.org/72399, http://www.php.net/ChangeLog-5.php, http://en.securitylab.ru/nvd/426726.php, http://secunia.com/advisories/cve_reference/CVE-2012-2386

2.39 - PHP Remote Code Execution and Denail of Service Vulnerabilities Dec13

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

10.0.7.45(TDDESKTOP-DT)

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 (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 Denail of Service Vulnerabilities Dec13 (OID: 1.3.6.1.4.1.25623.1.0.804174) Version used: $Revision: 143 $

Product Detection Result

Product: cpe:/a:php:php:5.3.8 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References

http://www.osvdb.com/100979, http://secunia.com/advisories/56055, http://packetstormsecurity.com/files/124436/PHP-openssl_x509_parse-Memory-Corruption.html

2.40 - PHP XML Handling Heap Buffer Overflow Vulnerability July13 (Windows)

Medium (CVSS: 6.8) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.803729

Summary

This host is running PHP and is prone to heap based buffer overflow vulnerability.
Affected Nodes 10.0.7.45(TDDESKTOP-DT)
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow attackers to cause a heap-based buffer overflow, resulting in a denial of service or potentially allowing the execution of arbitrary code.
Solution Upgrade to PHP version 5.3.27 or later, For updates refer to http://php.net/
Vulnerability Insight The flaw is triggered as user-supplied input is not properly validated when handling malformed XML input.
Vulnerability Detection Method Get the installed version of PHP with the help of detect NVT and check it is vulnerable or not. Details: PHP XML Handling Heap Buffer Overflow Vulnerability July13 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803729) Version used: $Revision: 11 $
References http://www.osvdb.org/95152, http://php.net/ChangeLog-5.php, https://bugs.php.net/bug.php?id=65236, http://seclists.org/oss-sec/2013/q3/88, http://seclists.org/bugtraq/2013/Jul/106

2.41 - PHP Sessions Subsystem Session Fixation Vulnerability-Aug13 (Windows)

Medium (CVSS: 6.8) OID: 1.3.6.1.4.1.25623.1.0.803737	80/tcp (http)
Summary This host is running PHP and is prone to session fixation vulnerability.	
Affected Nodes 10.0.7.45(TDDESKTOP-DT)	
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.	
Impact Successful exploitation will allow attackers to hijack web sessions by specifying a session ID.	
Solution Upgrade to PHP version 5.5.2 or later, For updates refer to http://php.net	
Vulnerability Insight PHP contains an unspecified flaw in the Sessions subsystem.	

Vulnerability Detection Method

Get the installed version of PHP with the help of detect NVT and check it is vulnerable or not. Details: PHP Sessions Subsystem Session Fixation Vulnerability-Aug13 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803737) Version used: $Revision: 11 $

References

http://www.osvdb.org/96316, http://secunia.com/advisories/54562, http://cxsecurity.com/cveshow/CVE-2011-4718, http://git.php.net/?p=php-src.git;a=commit;h=169b78eb79b0e080b67f9798708eb3771c6d0b2f, http://git.php.net/?p=php-src.git;a=commit;h=25e8fcc88fa20dc9d4c47184471003f436927cde

2.42 - PHP Multiple Vulnerabilities -01 Marcush13 (Windows)

Medium (CVSS: 5.8) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.803341

Summary

This host is running PHP and is prone to multiple vulnerabilities.

Affected Nodes

10.0.7.45(TDDESKTOP-DT)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow attackers to retrieve, corrupt or upload arbitrary files, or can cause denial of service via corrupted $_FILES indexes. Impact Level: Application

Solution

Upgrade to PHP 5.4.0 or later For updates refer to http://www.php.net/downloads.php

Vulnerability Insight

Flaw due to insufficient validation of file-upload implementation in rfc1867.c and it does not handle invalid '[' characters in name values.

Vulnerability Detection Method

Details: PHP Multiple Vulnerabilities -01 Marcush13 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803341) Version used: $Revision: 81 $

References

http://www.php.net/ChangeLog-5.php, http://cxsecurity.com/cveshow/CVE-2012-1172, http://secunia.com/advisories/cve_reference/CVE-2012-1172

2.43 - Apache HTTP Server mod_proxy_ajp Process Timeout DoS Vulnerability (Windows)

Medium (CVSS: 5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.802683

Summary

The host is running Apache HTTP Server and is prone to denial of service vulnerability.

Affected Nodes

10.0.7.45(TDDESKTOP-DT)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation could allow remote attackers to cause a denial of service condition via an expensive request. Impact Level: Application

Solution

Apply patch or upgrade Apache HTTP Server 2.2.22 or later, For updates refer to http://svn.apache.org/viewvc?view=revision&revision=1227298 ***** NOTE: Ignore this warning, if above mentioned patch is manually applied. *****

Vulnerability Insight

The flaw is due to an error in the mod_proxy_ajp module, which places a worker node into an error state upon detection of a long request-processing time.

Vulnerability Detection Method

Details: Apache HTTP Server mod_proxy_ajp Process Timeout DoS Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.802683) Version used: $Revision: 12 $

Product Detection Result

Product: cpe:/a:apache:http_server:2.2.21 Method: Apache Web Server Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

References

https://bugzilla.redhat.com/show_bug.cgi?id=871685, http://httpd.apache.org/security/vulnerabilities_22.html#2.2.22, http://svn.apache.org/viewvc?view=revision&revision=1227298

2.44 - PHP open_basedir Secuirity Bypass Vulnerability (Windows)

Medium (CVSS: 5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.803318

Summary

This host is running PHP and is prone to security bypass vulnerability.

Affected Nodes

10.0.7.45(TDDESKTOP-DT)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation could allow attackers to bypass certain security restrictions. Impact Level: Application

Solution

upgrade to PHP 5.3.15 or later For updates refer to http://www.php.net/downloads.php

Vulnerability Insight

Flaw in SQLite functionality allows attackers to bypass the open_basedir protection mechanism.

Vulnerability Detection Method

Details: PHP 'open_basedir' Secuirity Bypass Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803318) Version used: $Revision: 81 $

References

http://www.php.net/ChangeLog-5.php, http://en.securitylab.ru/nvd/427459.php, http://secunia.com/advisories/cve_reference/CVE-2012-3365

2.45 - PHP Multiple Vulnerabilities - June13 (Windows)

Medium (CVSS: 5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.803678

Summary

This host is running PHP and is prone to multiple vulnerabilities.

Affected Nodes

10.0.7.45(TDDESKTOP-DT)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation allows attackers to execute arbitrary code or cause denial of service condition via crafted arguments. Impact Level:System/ Application

Solution

Upgrade to PHP 5.4.16 or 5.3.26 or later, For updates refer to http://www.php.net/downloads.php

Vulnerability Insight

Multiple flaws are due to, - Heap-based overflow in 'php_quot_print_encode' function in 'ext/standard/quot_print.c' script. - Integer overflow in the 'SdnToJewish' function in 'jewish.c' in the Calendar component.

Vulnerability Detection Method

Details: PHP Multiple Vulnerabilities - June13 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803678) Version used: $Revision: 81 $

References

http://www.php.net/ChangeLog-5.php, http://bugs.php.net/bug.php?id=64895, http://bugs.php.net/bug.php?id=64879, http://www.security-database.com/detail.php?alert=CVE-2013-4635, http://www.security-database.com/detail.php?alert=CVE-2013-2110

2.46 - PHP open_basedir Security Bypass Vulnerability

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

OID: 1.3.6.1.4.1.25623.1.0.804241

Summary

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

Affected Nodes

10.0.7.45(TDDESKTOP-DT)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

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: 1022 $

Product Detection Result

Product: cpe:/a:php:php:5.3.8 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

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

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

10.0.7.45(TDDESKTOP-DT)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

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: 520 $

Product Detection Result

Product: cpe:/a:php:php:5.3.8 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References

http://osvdb.com/107560, http://osvdb.com/107559, http://www.php.net/ChangeLog-5.php, http://secunia.com/advisories/58804, https://www.hkcert.org/my_url/en/alert/14060401

2.48 - PHP SSL Certificate Validation Security Bypass Vulnerability (Windows)

Medium (CVSS: 4.3) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.803739

Summary

This host is running PHP and is prone to security bypass vulnerability.

Affected Nodes

10.0.7.45(TDDESKTOP-DT)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to spoof the server via a MitM (Man-in-the-Middle) attack and disclose potentially sensitive information.

Solution

Upgrade to PHP version 5.4.18 or 5.5.2 or later, For updates refer to http://php.net

Vulnerability Insight

The flaw is due to the SSL module not properly handling NULL bytes inside 'subjectAltNames' general names in the server SSL certificate.

Vulnerability Detection Method

Get the installed version of PHP with the help of detect NVT and check it is vulnerable or not. Details: PHP SSL Certificate Validation Security Bypass Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803739) Version used: $Revision: 113 $

References

http://www.osvdb.com/96298, http://secunia.com/advisories/54480, http://www.php.net/ChangeLog-5.php, http://git.php.net/?p=php-src.git;a=commit;h=2874696a5a8d46639d261571f915c493cd875897

2.49 - PHP SOAP Parser Multiple Information Disclosure Vulnerabilities

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

10.0.7.45(TDDESKTOP-DT)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

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: 98 $

Product Detection Result

Product: cpe:/a:php:php:5.3.8 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References

http://www.osvdb.org/90922, http://php.net/ChangeLog-5.php, http://git.php.net/?p=php-src.git;a=commit;h=afe98b7829d50806559acac9b530acb8283c3bf4

2.50 - PHP LibGD Denial of Service Vulnerability

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

Summary

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

Affected Nodes

10.0.7.45(TDDESKTOP-DT)
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
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: 642 $
Product Detection Result Product: cpe:/a:php:php:5.3.8 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)
References http://www.osvdb.com/104502, https://bugs.php.net/bug.php?id=66901

2.51 - Apache HTTP Server httpOnly Cookie Information Disclosure Vulnerability

Medium (CVSS: 4.3) OID: 1.3.6.1.4.1.25623.1.0.902830	80/tcp (http)
Summary This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.	
Affected Nodes 10.0.7.45(TDDESKTOP-DT)	
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.	
Impact Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks. Impact Level: Application	
Solution Upgrade to Apache HTTP Server version 2.2.22 or later, For updates refer to http://httpd.apache.org/	
Vulnerability Insight The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.	

Vulnerability Detection Method

Details: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902830) Version used: $Revision: 347 $

References

http://osvdb.org/78556, http://secunia.com/advisories/47779, http://www.exploit-db.com/exploits/18442, http://rhn.redhat.com/errata/RHSA-2012-0128.html, http://httpd.apache.org/security/vulnerabilities_22.html, http://svn.apache.org/viewvc?view=revision&revision=1235454, http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html

2.52 - PHP Information Disclosure Vulnerability-01 Sep14

Low (CVSS: 2.6) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.804849

Summary

This host is installed with PHP and is prone to information disclosure vulnerability.

Affected Nodes

10.0.7.45(TDDESKTOP-DT)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

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: 787 $

Product Detection Result

Product: cpe:/a:php:php:5.3.8 Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)

References

http://www.osvdb.com/108468, 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

2.53 - Microsoft IIS FTPd NLST stack overflow

High (CVSS: 9.3) 21/tcp (ftp)
OID: 1.3.6.1.4.1.25623.1.0.100952

Summary

Microsoft IIS FTPd NLST stack overflow The Microsoft IIS FTPd service may be vulnerable to a stack overflow via the NLST command. On Microsoft IIS 5.x this vulnerability can be used to gain remote SYSTEM level access, whilst on IIS 6.x it has been reported to result in a denial of service. Whilst it can be triggered by authenticated users with write access to the FTP server, this check determines whether anonymous users have the write access necessary to trigger it without authentication. On the following platforms, we recommend you mitigate in the described manner: Microsoft IIS 5.x Microsoft IIS 6.x We recommend you mitigate in the following manner: Filter inbound traffic to 21/tcp to only known management hosts Consider removing directories writable by 'anonymous'

Affected Nodes

10.0.7.65(MYCO30DEV)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

We are not aware of a vendor approved solution at the current time.

Vulnerability Detection Method

Details: Microsoft IIS FTPd NLST stack overflow (OID: 1.3.6.1.4.1.25623.1.0.100952) Version used: $Revision: 15 $

References

http://www.securityfocus.com/bid/36189

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

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

10.0.7.65(MYCO30DEV)

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 user 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: 174 $

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

2.55 - Windows Administrator NULL FTP password

High (CVSS: 9) 21/tcp (ftp)
OID: 1.3.6.1.4.1.25623.1.0.11160

Summary

The remote server is incorrectly configured with a NULL password for the user 'Administrator' and has FTP enabled.

Affected Nodes

10.0.7.65(MYCO30DEV)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

Change the Administrator password on this host.

Vulnerability Detection Method

Details: Windows Administrator NULL FTP password (OID: 1.3.6.1.4.1.25623.1.0.11160) Version used: $Revision: 17 $

2.56 - Apache Tomcat servlet/JSP container default files

Medium (CVSS: 6.8) 8080/tcp (http-alt)
OID: 1.3.6.1.4.1.25623.1.0.12085

Summary

The Apache Tomcat servlet/JSP container has default files installed. These files should be removed as they may help an attacker to guess the exact version of the Apache Tomcat which is running on this host and may provide other useful information.

Affected Nodes

10.0.7.65(MYCO30DEV)

Vulnerability Detection Result

Default files, such as documentation, default Servlets and JSPs were found on the Apache Tomcat servlet/JSP container. Remove default files, example JSPs and Servlets from the Tomcat Servlet/JSP container. These files should be removed as they may help an attacker to guess the exact version of Apache Tomcat which is running on this host and may provide other useful information. The following default files were found : /tomcat-docs/index.html /examples/servlets/index.html /examples/jsp/snp/snoop.jsp /examples/jsp/index.html

Vulnerability Detection Method

Details: Apache Tomcat servlet/JSP container default files (OID: 1.3.6.1.4.1.25623.1.0.12085) Version used: $Revision: 17 $

2.57 - Apache Tomcat Multiple Vulnerabilities - 01 Mar14

Medium (CVSS: 5.8) 8080/tcp (http-alt)
OID: 1.3.6.1.4.1.25623.1.0.804519

Summary

This host is running Apache Tomcat and is prone to multiple vulnerabilities.

Affected Nodes

10.0.7.65(MYCO30DEV)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to conduct session fixation attacks and manipulate certain data. Impact Level: Application

Solution

Upgrade to version 6.0.39 or 7.0.47 or 8.0.0-RC3 or later, For Updates refer to http://tomcat.apache.org

Vulnerability Insight

Flaws are due to the HTTP connector or AJP connector which do not properly handle certain inconsistent HTTP request headers.

Vulnerability Detection Method

Get the installed version of Apache Tomcat with the help of detect NVT and check the version is vulnerable or not. Details: Apache Tomcat Multiple Vulnerabilities - 01 Mar14 (OID: 1.3.6.1.4.1.25623.1.0.804519) Version used: $Revision: 359 $

Product Detection Result

Product: cpe:/a:apache:tomcat:4.1.27 Method: Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)

References

http://www.osvdb.com/103708, http://seclists.org/bugtraq/2014/Feb/134, http://packetstormsecurity.com/files/125394

2.58 - IIS Service Pack - 404

Medium (CVSS: 5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.11874

Summary

The Patch level (Service Pack) of the remote IIS server appears to be lower than the current IIS service pack level. As each service pack typically contains many security patches, the server may be at risk. Caveat: This test makes assumptions of the remote patch level based on static return values (Content-Length) within the IIS Servers 404 error message. As such, the test can not be totally reliable and should be manually confirmed.

Affected Nodes

10.0.7.65(MYCO30DEV)

Vulnerability Detection Result

The remote IIS server *seems* to be Microsoft IIS 5 - SP3 or SP4

Solution

Ensure that the server is running the latest stable Service Pack

Vulnerability Detection Method

Details: IIS Service Pack - 404 (OID: 1.3.6.1.4.1.25623.1.0.11874) Version used: $Revision: 982 $

2.59 - Microsoft ASP.NET Information Disclosure Vulnerability (2418042)

Medium (CVSS: 5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.901161

Summary

This host is missing a critical security update according to Microsoft Bulletin MS10-070.

Affected Nodes

10.0.7.65(MYCO30DEV)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation could allow remote attackers to decrypt and gain access to potentially sensitive data encrypted by the server or read data from arbitrary files within an ASP.NET application. Obtained information may aid in further attacks.
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/MS10-070.mspx

Vulnerability Insight

The flaw is due to an error within ASP.NET in the handling of cryptographic padding when using encryption in CBC mode. This can be exploited to decrypt data via returned error codes from an affected server.

Vulnerability Detection Method

Details: Microsoft ASP.NET Information Disclosure Vulnerability (2418042) (OID: 1.3.6.1.4.1.25623.1.0.901161) Version used: $Revision: 14 $

References

http://www.vupen.com/english/advisories/2010/2429, http://www.microsoft.com/technet/security/bulletin/MS10-070.mspx, http://www.troyhunt.com/2010/09/fear-uncertainty-and-and-padding-oracle.html, http://weblogs.asp.net/scottgu/archive/2010/09/18/important-asp-net-security-vulnerability.aspx

2.60 - Microsoft IIS IP Address/Internal Network Name Disclosure Vulnerability

Medium (CVSS: 5) 80/tcp (http)
OID: 1.3.6.1.4.1.25623.1.0.902796

Summary

The host is running Microsoft IIS Webserver and is prone to IP address disclosure vulnerability.

Affected Nodes

10.0.7.65(MYCO30DEV)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to gain internal IP address or internal network name, which could assist in further attacks against the target host. Impact Level: Application

Solution

Apply the hotfix for IIS 6.0 from below link http://support.microsoft.com/kb/834141/#top

Vulnerability Insight

The flaw is due to an error while processing 'GET' request. When MS IIS receives a GET request without a host header, the Web server will reveal the IP address of the server in the content-location field or the location field in the TCP header in the response.

Vulnerability Detection Method

Details: Microsoft IIS IP Address/Internal Network Name Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902796) Version used: $Revision: 12 $

References

http://support.microsoft.com/kb/834141/, http://www.securityfocus.com/bid/3159/info, http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q218180, http://www.juniper.net/security/auto/vulnerabilities/vuln3159.html

2.61 - Apache Tomcat Multiple Vulnerabilities June-09

Medium (CVSS: 5) 8080/tcp (http-alt)
OID: 1.3.6.1.4.1.25623.1.0.800813

Summary

This host is running Apache Tomcat Server and is prone to multiple vulnerabilities.

Affected Nodes

10.0.7.65(MYCO30DEV)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful attempt could lead to remote code execution and attacker can gain the full permission on affected file, and can cause denial of service. Impact Level: System/Application

Solution

Upgrade to Apache Tomcat version 4.1.40, or 5.5.28, or 6.0.20 http://archive.apache.org/dist/tomcat/

Vulnerability Insight

Multiple flows are due to, - Error in 'XML parser' used for other web applications, which allows local users to read or modify the web.xml, context.xml, or tld files via a crafted application that is loaded earlier than the target application. - when FORM authentication is used, cause enumerate valid usernames via requests to /j_security_check with malformed URL encoding of passwords, related to improper error checking in the MemoryRealm, DataSourceRealm, and JDBCRealm authentication realms, as demonstrated by a % (percent) value for the j_password parameter. - when the 'Java AJP connector' and 'mod_jk load balancing' are used, via a crafted request with invalid headers, related to temporary blocking of connectors that have encountered errors, as demonstrated by an error involving a malformed HTTP Host header.

Vulnerability Detection Method

Details: Apache Tomcat Multiple Vulnerabilities June-09 (OID: 1.3.6.1.4.1.25623.1.0.800813) Version used: $Revision: 15 $

Product Detection Result

Product: cpe:/a:apache:tomcat:4.1.27 Method: Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)

References

http://tomcat.apache.org/security-6.html, http://tomcat.apache.org/security-5.html, http://tomcat.apache.org/security-4.html, http://www.securitytracker.com/id?1022336, http://www.vupen.com/english/advisories/2009/1496, http://svn.apache.org/viewvc?view=rev&revision=781708

2.62 - Apache Tomcat Cross-Site Scripting and Security Bypass Vulnerabilities

Medium (CVSS: 5) 8080/tcp (http-alt)
OID: 1.3.6.1.4.1.25623.1.0.900021

Summary

This host is running Apache Tomcat web server, which is prone to cross site scripting and security bypass vulnerabilities.

Affected Nodes

10.0.7.65(MYCO30DEV)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation could cause execution of arbitrary HTML code, script code, and information disclosure. Impact Level : Application.

Solution

Upgrade to higher version of 4.x, 5.x, or 6.x series. http://tomcat.apache.org/

Vulnerability Insight

The flaws are due to, - input validation error in the method HttpServletResponse.sendError() which fails to properly sanitise before being returned to the user in the HTTP Reason-Phrase. - the application fails to normalize the target path before removing the query string when using a RequestDispatcher.
Vulnerability Detection Method Details: Apache Tomcat Cross-Site Scripting and Security Bypass Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.900021) Version used: $Revision: 16 $
References http://secunia.com/advisories/31379/, http://secunia.com/advisories/31381/

2.63 - Microsoft IIS Default Welcome Page Information Disclosure Vulnerability

Medium (CVSS: 4.6) 80/tcp (http) OID: 1.3.6.1.4.1.25623.1.0.802806
Summary The host is running Microsoft IIS Webserver and is prone to information disclosure vulnerability.
Affected Nodes 10.0.7.65(MYCO30DEV)
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 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 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: 308 $
References http://www.iis.net/, http://osvdb.org/2117

2.64 - Apache Tomcat JSP Example Web Applications Cross Site Scripting Vulnerability

Medium (CVSS: 4.3)	8080/tcp (http-alt)
OID: 1.3.6.1.4.1.25623.1.0.111014	

Summary

This host is running Apache Tomcat and is prone to Cross Site Scripting vulnerability.

Affected Nodes

10.0.7.65(MYCO30DEV)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Exploiting this vulnerability may allow an attacker to perform cross-site scripting attacks on unsuspecting users in the context of the affected website. As a result, the attacker may be able to steal cookie-based authentication credentials and to launch other attacks.

Solution

Update your Apache Tomcat to a non-affected version.

Vulnerability Detection Method

Details: Apache Tomcat JSP Example Web Applications Cross Site Scripting Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.111014) Version used: $Revision: 1173 $

Product Detection Result

Product: cpe:/a:apache:tomcat:4.1.27 Method: Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)

References

http://www.securityfocus.com/bid/24476/, http://tomcat.apache.org/security-6.html, http://tomcat.apache.org/security-5.html, http://tomcat.apache.org/security-4.html

2.65 - Apache Tomcat RemoteFilterValve Security Bypass Vulnerability

Medium (CVSS: 4.3)	8080/tcp (http-alt)
OID: 1.3.6.1.4.1.25623.1.0.800024	

Summary

Apache Tomcat Server is running on this host and that is prone to security bypass vulnerability.

Affected Nodes

10.0.7.65(MYCO30DEV)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful attempt could lead to remote code execution and attacker can gain access to context of the filtered value. Impact Level: Application

Solution

Upgrade to Apache Tomcat version 4.1.32, or 5.5.1, or later, http://archive.apache.org/dist/tomcat/

Vulnerability Insight

Flaw in the application is due to the synchronisation problem when checking IP addresses. This could allow user from a non permitted IP address to gain access to a context that is protected with a valve that extends RemoteFilterValve including the standard RemoteAddrValve and RemoteHostValve implementations.

Vulnerability Detection Method

Details: Apache Tomcat RemoteFilterValve Security Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.800024) Version used: $Revision: 16 $

References

http://tomcat.apache.org/security-4.html, http://tomcat.apache.org/security-5.html, https://issues.apache.org/bugzilla/show_bug.cgi?id=25835

2.66 - Apache Tomcat Multiple Vulnerabilities - 02 Mar14

Medium (CVSS: 4.3) 8080/tcp (http-alt)
OID: 1.3.6.1.4.1.25623.1.0.804520

Summary

This host is running Apache Tomcat and is prone to multiple vulnerabilities.

Affected Nodes

10.0.7.65(MYCO30DEV)

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to gain access to potentially sensitive internal information or crash the program. Impact Level: Application

Solution

Upgrade to version 6.0.39 or 7.0.50 or 8.0.0-RC10 or later, For Updates refer to http://tomcat.apache.org

Vulnerability Insight

Multiple flaws are due to, - Error when handling a request for specially crafted malformed header (i.e. whitespace after the : in a trailing header). - Improper parsing of XML data to an incorrectly configured XML parser accepting XML external entities from an untrusted source.

Vulnerability Detection Method

Get the installed version of Apache Tomcat with the help of detect NVT and check the version is vulnerable or not. Details: Apache Tomcat Multiple Vulnerabilities - 02 Mar14 (OID: 1.3.6.1.4.1.25623.1.0.804520) Version used: $Revision: 391 $

Product Detection Result

Product: cpe:/a:apache:tomcat:4.1.27 Method: Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)

References

http://www.osvdb.com/103706, http://www.osvdb.com/103707, http://seclists.org/bugtraq/2014/Feb/132, http://seclists.org/bugtraq/2014/Feb/133, http://packetstormsecurity.com/files/125400, http://packetstormsecurity.com/files/125404

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

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

Summary

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

Affected Nodes

10.0.7.68(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: 14 $

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

2.68 - Microsoft Windows SMTP Server DNS spoofing vulnerability

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

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 network traffic and to launch man-in-the-middle attacks.

Affected Nodes

10.0.7.68(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: 701 $

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

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

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

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 users. Attackers can exploit the information-disclosure issue to gain access to sensitive information. Any information obtained may lead to further attacks.

Affected Nodes

10.0.7.68(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: 14 $

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