Nessus Report

Report

21/Mar/2012:16:43:56 GMT

Table Of Contents

Vulnerabilities By Host

192.168.150.100

Scan Information

Start time:	Wed Mar 21 14:40:36 2012
End time:	Wed Mar 21 15:01:02 2012

Host Information

Netbios Name:	WINDOWS2000
IP:	192.168.150.100
MAC Address:	00:0c:29:f7:55:ea
OS:	Microsoft Windows 2000 Service Pack 4

Results Summary

Critical	High	Medium	Low	Info	Total
14	2	5	0	3	24

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS

Synopsis

It may be possible to send spoofed RST packets to the remote system.

Description

The remote host might be vulnerable to a sequence number approximation bug, which may allow an attacker to send spoofed RST packets to the remote host and close established connections. This may cause problems for some dedicated services (BGP, a VPN over TCP, etc...).

Solution

See http://www.securityfocus.com/bid/10183/solution/

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

4.1 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

BID	10183
CVE	CVE-2004-0230
XREF	OSVDB:4030
XREF	IAVA:2004-A-0007

Ports

tcp/0

25/tcp

45517 - MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832) (uncredentialed check)

Synopsis

The remote mail server may be affected by multiple vulnerabilities.

Description

The installed version of Microsoft Exchange / Windows SMTP Service is affected by at least one vulnerability :
- Incorrect parsing of DNS Mail Exchanger (MX) resource records could cause the Windows Simple Mail Transfer Protocol (SMTP) component to stop responding until the service is restarted. (CVE-2010-0024)
- Improper allocation of memory for interpreting SMTP command responses may allow an attacker to read random e-mail message fragments stored on the affected server.
(CVE-2010-0025)

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, and 2008 as well as Exchange Server 2000, 2003, 2007, and 2010 :
http://technet.microsoft.com/en-us/security/bulletin/MS10-024

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

BID	39381
CVE	CVE-2010-0024
CVE	CVE-2010-0025
XREF	OSVDB:63738
XREF	OSVDB:63739
XREF	MSFT:MS10-024

Exploitable with

Core Impact (true)

Ports

tcp/25

```
The remote version of the smtpsvc.dll is 5.0.2195.6713 versus 5.0.2195.7381.
```

80/tcp

10357 - Microsoft IIS MDAC RDS (msadcs.dll) Arbitrary Remote Command Execution

Synopsis

The remote web server is affected by a remote command execution vulnerability.

Description

The web server is probably susceptible to a common IIS vulnerability discovered by 'Rain Forest Puppy'. This vulnerability enables an attacker to execute arbitrary commands on the server with Administrator Privileges.
*** Nessus solely relied on the presence of the file /msadc/msadcs.dll
*** so this might be a false positive

See Also

http://support.microsoft.com/default.aspx?scid=kb;[LN];184375

http://technet.microsoft.com/en-us/security/bulletin/ms98-004

http://technet.microsoft.com/en-us/security/bulletin/ms99-025

Solution

Upgrade to MDAC version 2.1 SP2 or higher, as it has been reported to fix this vulnerability. It is also possible to correct the flaw by implementing the following workaround: Delete the /msadc virtual directory in IIS.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

9.5 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	529
CVE	CVE-1999-1011
XREF	OSVDB:272
XREF	CWE:264
XREF	MSFT:MS98-004
XREF	MSFT:MS99-025

Ports

tcp/80

11161 - Microsoft Data Access Components RDS Data Stub Remote Overflow

Synopsis

The remote host is affected by a remote buffer overflow vulnerability.

Description

The remote DLL /msadc/msadcs.dll is accessible by anyone. Several flaws have been found in it in the past. We recommend that you restrict access to MSADC only to trusted hosts.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms02-065

http://archives.neohapsis.com/archives/vulnwatch/2002-q4/0082.html

Solution

- Launch the Internet Services Manager
- Select your web server
- Right-click on MSADC and select 'Properties'
- Select the tab 'Directory Security'
- Click on the 'IP address and domain name restrictions'
option
- Make sure that by default, all computers are DENIED access to this resource
- List the computers that should be allowed to use it

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	6214
CVE	CVE-2002-1142
XREF	OSVDB:14502
XREF	IAVA:2002-A-0005
XREF	MSFT:MS02-065

Ports

tcp/80

```
*** Nessus did not test for any security vulnerability but solely relied
*** on the presence of this resource to issue this warning, so this
*** might be a false positive.
```

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

http://www.kb.cert.org/vuls/id/288308

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

http://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.9 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:5648
XREF	OSVDB:50485
XREF	CWE:16

Ports

tcp/80

```
Use the URLScan tool to deny HTTP TRACE requests or to permit only the
methods needed to meet site requirements and policy.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus1444844647.html HTTP/1.1
Connection: Close
Host: 192.168.150.100
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 21 Mar 2012 17:45:29 GMT
Content-Type: message/http
Content-Length: 317


TRACE /Nessus1444844647.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.150.100
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1 [...]
```

135/udp

11890 - MS03-043: Buffer Overrun in Messenger Service (828035) (uncredentialed check)

Synopsis

Arbitrary code can be executed on the remote host.

Description

A security vulnerability exists in the Messenger Service that could allow arbitrary code execution on an affected system. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system or could cause the Messenger Service to fail.
Disabling the Messenger Service will prevent the possibility of attack.
This plugin actually tests for the presence of this flaw.

Solution

Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 :
http://technet.microsoft.com/en-us/security/bulletin/ms03-043

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	8826
CVE	CVE-2003-0717
XREF	OSVDB:10936
XREF	IAVA:2003-A-0017
XREF	MSFT:MS03-043

Exploitable with

CANVAS (true)

Ports

udp/135

445/tcp

22194 - MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)

Synopsis

Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description

The remote host is vulnerable to a buffer overrun in the 'Server'
service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges.

Solution

Microsoft has released a set of patches for Windows 2000, XP and 2003 :
http://technet.microsoft.com/en-us/security/bulletin/ms06-040

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.7 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	19409
CVE	CVE-2006-3439
XREF	OSVDB:27845
XREF	IAVA:2006-A-0036
XREF	MSFT:MS06-040

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

19408 - MS05-039: Vulnerability in Plug and Play Service Could Allow Remote Code Execution (899588) (uncredentialed check)

Synopsis

Arbitrary code can be executed on the remote host due to a flaw in the Plug-And-Play service.

Description

The remote version of Windows contains a flaw in the function 'PNP_QueryResConfList()' in the Plug and Play service
that may allow an attacker to execute arbitrary code on the remote host with SYSTEM privileges.
A series of worms (Zotob) are known to exploit this vulnerability in the wild.

Solution

Microsoft has released a set of patches for Windows 2000, XP and 2003 :
http://technet.microsoft.com/en-us/security/bulletin/ms05-039

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	14513
CVE	CVE-2005-1983
XREF	OSVDB:18605
XREF	IAVA:2005-A-0025
XREF	MSFT:MS05-039

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

21193 - MS05-047: Plug and Play Remote Code Execution and Local Privilege Elevation (905749) (uncredentialed check)

Synopsis

A flaw in the Plug and Play service may allow an authenticated attacker to execute arbitrary code on the remote host and, therefore, elevate his privileges.

Description

The remote host contains a version of the Plug and Play service that contains a vulnerability in the way it handles user-supplied data.
An authenticated attacker may exploit this flaw by sending a malformed RPC request to the remote service and execute code with SYSTEM privileges.
Note that authentication is not required against Windows 2000 if the MS05-039 patch is missing.

Solution

Microsoft has released a set of patches for Windows 2000 and XP :
http://technet.microsoft.com/en-us/security/bulletin/ms05-047

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	15065
CVE	CVE-2005-2120
XREF	OSVDB:18830
XREF	MSFT:MS05-047

Exploitable with

Core Impact (true)

Ports

tcp/445

18502 - MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)

Synopsis

Arbitrary code can be executed on the remote host due to a flaw in the SMB implementation.

Description

The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation that may allow an attacker to execute arbitrary code on the remote host.
An attacker does not need to be authenticated to exploit this flaw.

Solution

Microsoft has released a set of patches for Windows 2000, XP and 2003 :
http://technet.microsoft.com/en-us/security/bulletin/ms05-027

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	13942
CVE	CVE-2005-1206
XREF	OSVDB:17308
XREF	MSFT:MS05-027

Exploitable with

Core Impact (true)

Ports

tcp/445

19407 - MS05-043: Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) (uncredentialed check)

Synopsis

Arbitrary code can be executed on the remote host due to a flaw in the Spooler service.

Description

The remote host contains a version of the Print Spooler service that may allow an attacker to execute code on the remote host or crash the spooler service.
An attacker can execute code on the remote host with a NULL session against :
- Windows 2000
An attacker can crash the remote service with a NULL session against :
- Windows 2000
- Windows XP SP1
An attacker needs valid credentials to crash the service against :
- Windows 2003
- Windows XP SP2

Solution

Microsoft has released a set of patches for Windows 2000, XP and 2003 :
http://technet.microsoft.com/en-us/security/bulletin/ms05-043

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	14514
CVE	CVE-2005-1984
XREF	OSVDB:18607
XREF	MSFT:MS05-043

Exploitable with

CANVAS (true)Core Impact (true)

Ports

tcp/445

11835 - MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed check)

Synopsis

Arbitrary code can be executed on the remote host.

Description

The remote host is running a version of Windows that has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges.
An attacker or a worm could use it to gain the control of this host.
Note that this is NOT the same bug as the one described in MS03-026, which fixes the flaw exploited by the 'MSBlast' (or LoveSan) worm.

Solution

http://technet.microsoft.com/en-us/security/bulletin/ms03-039

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	8458
BID	8460
CVE	CVE-2003-0715
CVE	CVE-2003-0528
CVE	CVE-2003-0605
XREF	OSVDB:11460
XREF	OSVDB:11797
XREF	OSVDB:2535
XREF	IAVA:2003-A-0012
XREF	MSFT:MS03-039

Ports

tcp/445

12209 - MS04-011: Security Update for Microsoft Windows (835732) (uncredentialed check)

Synopsis

Arbitrary code can be executed on the remote host due to a flaw in the LSASS service.

Description

The remote version of Windows contains a flaw in the function 'DsRolerUpgradeDownlevelServer' of the Local Security Authority Server Service (LSASS) that may allow an attacker to execute arbitrary code on the remote host with SYSTEM privileges.
A series of worms (Sasser) are known to exploit this vulnerability in the wild.

Solution

Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 :
http://technet.microsoft.com/en-us/security/bulletin/ms04-011

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	10108
CVE	CVE-2003-0533
XREF	OSVDB:5248
XREF	IAVA:2004-A-0006
XREF	MSFT:MS04-011

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

12054 - MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028) (uncredentialed check)

Synopsis

Arbitrary code can be executed on the remote host.

Description

The remote Windows host has an ASN.1 library that could allow an attacker to execute arbitrary code on this host.
To exploit this flaw, an attacker would need to send a specially crafted ASN.1 encoded packet with improperly advertised lengths.
This particular check sent a malformed NTLM packet and determined that the remote host is not patched.

Solution

http://technet.microsoft.com/en-us/security/bulletin/ms04-007

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	9633
BID	9635
BID	9743
BID	13300
CVE	CVE-2003-0818
XREF	OSVDB:3902
XREF	IAVA:2004-A-0001
XREF	MSFT:MS04-007

Exploitable with

CANVAS (true)Metasploit (true)

Ports

tcp/445

11808 - MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncredentialed check)

Synopsis

Arbitrary code can be executed on the remote host.

Description

The remote version of Windows contains a flaw in the function RemoteActivation() in its RPC interface that could allow an attacker to execute arbitrary code on the remote host with the SYSTEM privileges.
A series of worms (Blaster) are known to exploit this vulnerability in the wild.

Solution

http://technet.microsoft.com/en-us/security/bulletin/ms03-026

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	8205
CVE	CVE-2003-0352
XREF	OSVDB:2100
XREF	IAVA:2003-A-0011
XREF	MSFT:MS03-026

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

34477 - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)

Synopsis

Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description

The remote host is vulnerable to a buffer overrun in the 'Server'
service that may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 :
http://technet.microsoft.com/en-us/security/bulletin/ms08-067

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.7 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	31874
CVE	CVE-2008-4250
XREF	OSVDB:49243
XREF	IAVA:2008-A-0081
XREF	MSFT:MS08-067
XREF	CWE:94

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Ports

tcp/445

22034 - MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)

Synopsis

Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description

The remote host is vulnerable to heap overflow in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges.
In addition to this, the remote host is also affected by an information disclosure vulnerability in SMB that may allow an attacker to obtain portions of the memory of the remote host.

Solution

Microsoft has released a set of patches for Windows 2000, XP and 2003 :
http://technet.microsoft.com/en-us/security/bulletin/ms06-035

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	18863
BID	18891
CVE	CVE-2006-1314
CVE	CVE-2006-1315
XREF	OSVDB:27154
XREF	OSVDB:27155
XREF	MSFT:MS06-035

Exploitable with

Core Impact (true)

Ports

tcp/445

56210 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials

Synopsis

It is possible to obtain the host SID for the remote host, without credentials.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier), without credentials.
The host SID can then be used to get the list of local users.

See Also

http://technet.microsoft.com/en-us/library/bb418944.aspx

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.
Refer to the 'See also' section for guidance.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

BID	959
CVE	CVE-2000-1200
XREF	OSVDB:715

Ports

tcp/445

```
The remote host SID value is :

1-5-21-1123561945-1085031214-839522115
```

56211 - SMB Use Host SID to Enumerate Local Users Without Credentials

Synopsis

It is possible to enumerate local users, without credentials.

Description

Using the host security identifier (SID), it is possible to enumerate local users on the remote Windows system without credentials.

Solution

n/a

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

BID	959
CVE	CVE-2000-1200
XREF	OSVDB:714

Ports

tcp/445

```
- Administrator (id 500, Administrator account)
- Guest (id 501, Guest account)
- IUSR_WINDOWS2000 (id 1000)
- IWAM_WINDOWS2000 (id 1001)
- paul (id 1002)
- kevin (id 1003)
- josh (id 1004)
- mike (id 1005)
- nessus (id 1006)
```

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It is possible to log into the remote host.

Description

The remote host is running Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :
- NULL session
- Guest account
- Given Credentials

See Also

http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP

http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

Solution

n/a

Risk Factor

None

Exploitable with

Metasploit (true)

Ports

tcp/445

```
- NULL sessions are enabled on the remote host
```

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).
The host SID can then be used to get the list of local users.

See Also

http://technet.microsoft.com/en-us/library/bb418944.aspx

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.
Refer to the 'See also' section for guidance.

Risk Factor

None

Ports

tcp/445

```
The remote host SID value is :
```

```
1-5-21-1123561945-1085031214-839522115

The value of 'RestrictAnonymous' setting is : unknown
```

10860 - SMB Use Host SID to Enumerate Local Users

Synopsis

It is possible to enumerate local users.

Description

Using the host security identifier (SID), it is possible to enumerate local users on the remote Windows system.

Solution

n/a

Risk Factor

None

Ports

tcp/445

```
  - Administrator (id 500, Administrator account)
  - Guest (id 501, Guest account)
  - IUSR_WINDOWS2000 (id 1000)
  - IWAM_WINDOWS2000 (id 1001)
  - paul (id 1002)
  - kevin (id 1003)
  - josh (id 1004)
  - mike (id 1005)
  - nessus (id 1006)

Note that, in addition to the Administrator and Guest accounts, Nessus
has enumerated only those local users with IDs between 1000 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for this plugin, then re-run the
scan.
```

1025/tcp

13852 - MS04-022: Microsoft Windows Task Scheduler Remote Overflow (841873) (uncredentialed check)

Synopsis

Arbitrary code can be executed on the remote host.

Description

There is a flaw in the Task Scheduler application which could allow a remote attacker to execute code remotely. There are many attack vectors for this flaw. An attacker, exploiting this flaw, would need to either have the ability to connect to the target machine or be able to coerce a local user to either install a .job file or browse to a malicious website.

Solution

Microsoft has released a set of patches for Windows 2000, XP and 2003 :
http://technet.microsoft.com/en-us/security/bulletin/ms04-022

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	10708
CVE	CVE-2004-0212
XREF	OSVDB:7798

XREF	IAVA:2004-A-0013
XREF	MSFT:MS04-022

Ports
tcp/1025

1210/tcp

21334 - MS06-018: Vulnerability in Microsoft Distributed Transaction Coordinator Could Allow DoS (913580) (uncredentialed check)

Synopsis
A vulnerability in MSDTC could allow remote code execution.

Description
The remote version of Windows contains a version of MSDTC (Microsoft Data Transaction Coordinator) service that is affected by several remote code execution and denial of service vulnerabilities.
An attacker may exploit these flaws to obtain complete control of the remote host (2000, NT4) or to crash the remote service (XP, 2003).

Solution
Microsoft has released a set of patches for Windows 2000, XP and 2003 :
http://technet.microsoft.com/en-us/security/bulletin/ms06-018

Risk Factor
Critical

CVSS Base Score
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References
BID	17905
BID	17906
CVE	CVE-2006-0034
CVE	CVE-2006-1184
XREF	OSVDB:25335
XREF	OSVDB:25336
XREF	MSFT:MS06-018

Exploitable with
Core Impact (true)

Ports
tcp/1210

192.168.150.131

Scan Information

Start time:	Wed Mar 21 14:40:36 2012
End time:	Wed Mar 21 16:43:56 2012

Host Information

IP:	192.168.150.131
MAC Address:	00:0c:29:16:e8:6c
OS:	Linux Kernel 2.6 on Ubuntu 9.10 (karmic)

Results Summary

Critical	High	Medium	Low	Info	Total
4	4	22	3	0	33

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS

Synopsis

It may be possible to send spoofed RST packets to the remote system.

Description

The remote host might be vulnerable to a sequence number approximation bug, which may allow an attacker to send spoofed RST packets to the remote host and close established connections. This may cause problems for some dedicated services (BGP, a VPN over TCP, etc...).

Solution

See http://www.securityfocus.com/bid/10183/solution/

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

4.1 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

BID	10183
CVE	CVE-2004-0230
XREF	OSVDB:4030
XREF	IAVA:2004-A-0007

Ports

tcp/0

56283 - Linux Kernel TCP Sequence Number Generation Security Weakness

Synopsis

It may be possible to predict TCP/IP Initial Sequence Numbers for the remote host.

Description

The Linux kernel is prone to a security weakness related to TCP sequence number generation. Attackers can exploit this issue to inject arbitrary packets into TCP sessions using a brute force attack.
An attacker may use this vulnerability to create a denial of service condition or a man-in-the-middle attack.
Note that this plugin may fire as a result of a network device (such as a load balancer, VPN, IPS, transparent proxy, etc.) that is vulnerable and that re-writes TCP sequence numbers, rather than the host itself being vulnerable.

See Also

http://lwn.net/Articles/455135/

http://www.nessus.org/u?9881d9af

Solution

Contact the OS vendor for a Linux kernel update / patch.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.6 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

References

BID	49289
CVE	CVE-2011-3188
XREF	OSVDB:75716

Ports

tcp/0

21/tcp

50544 - ProFTPD < 1.3.3c Multiple Vulnerabilities

Synopsis

The remote FTP server is affected by multiple vulnerabilities.

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.
According to its banner, the version of ProFTPD installed on the remote host is earlier than 1.3.3c. Such versions are reportedly affected by the following vulnerabilities :
- When ProFTPD is compiled with 'mod_site_misc' and a directory is writable, a user can use 'mod_site_misc' to create or delete a directory outside the writable directory, create a symlink located outside the writable directory, or change the time of a file located outside the writable directory. (Bug #3519)
- A stack-based buffer overflow exists in the server's 'pr_netio_telnet_gets()' function, which can be triggered by when reading user input containing a TELNET_IAC escape sequence. (Bug #3521)
Note that Nessus did not actually test for the flaws but instead has relied on the version in ProFTPD's banner so this may be a false positive.

See Also

http://www.zerodayinitiative.com/advisories/ZDI-10-229/

http://bugs.proftpd.org/show_bug.cgi?id=3519

http://bugs.proftpd.org/show_bug.cgi?id=3521

http://www.proftpd.org/docs/RELEASE_NOTES-1.3.3c

Solution

Upgrade to ProFTPD version 1.3.3c or later.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	44562
CVE	CVE-2010-3867
CVE	CVE-2010-4221
XREF	OSVDB:68985
XREF	OSVDB:68988
XREF	EDB-ID:15449
XREF	Secunia:42052

Exploitable with

Metasploit (true)

Ports

tcp/21

```
 Version source    : 220 ProFTPD 1.2.5 Server (ProFTPD Default Installation)
[SECURITYFAIL.localdomain]
 Installed version : 1.2.5
 Fixed version     : 1.3.3c
```

27055 - ProFTPD < 1.3.0a Multiple Vulnerabilities

Synopsis

The remote FTP server is affected by several vulnerabilities.

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.
According to its banner, the version of ProFTPD installed on the remote host is earlier than 1.3.0a. As such, it may be affected by one or more of the following vulnerabilities :
- An off-by-one string manipulation flaw exists in the 'sreplace' function. (CVE-2006-5815)
- A buffer overflow exists in the 'tls_x509_name_oneline' function of the mod_tls module involving the data length argument. (CVE-2006-6170)
- An off-by-two buffer overflow exists due to a failure to properly set the buffer size limit when 'CommandBufferSize' is specified in the configuration file, an issue which is disputed by the developers.
(CVE-2006-6171)
An attacker may be able to leverage this issue to crash the affected service or execute arbitrary code remotely, subject to the privileges under which the application operates.

See Also

http://archives.neohapsis.com/archives/bugtraq/2006-11/0095.html

http://www.securityfocus.com/archive/1/452760/30/0/threaded

Solution

Upgrade to ProFTPD version 1.3.0a or later.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	20992
CVE	CVE-2006-5815
CVE	CVE-2006-6170

CVE	CVE-2006-6171
XREF	OSVDB:30267
XREF	OSVDB:30660
XREF	OSVDB:30719
XREF	CWE:119

Exploitable with

Metasploit (true)

Ports

tcp/21

```
The banner reports this is ProFTPD version 1.2.5.
```

51366 - ProFTPD < 1.3.3d 'mod_sql' Buffer Overflow

Synopsis

The remote FTP server is affected by a heap-based buffer overflow vulnerability.

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.
According to its banner, the version of ProFTPD installed on the remote host is earlier than 1.3.3d. Such versions are reportedly affected by a heap-based buffer overflow vulnerability in the function 'sql_prepare_where()' in the file 'contrib/mod_sql.c'. An unauthenticated, remote attacker may be able to exploit this in combination with an earlier SQL injection vulnerability (CVE-2009-0542) to execute arbitrary code with root privileges.
Note that Nessus did not actually test for the flaw but instead has relied on the version in ProFTPD's banner.

See Also

http://phrack.org/issues.html?issue=67&id=7#article

http://bugs.proftpd.org/show_bug.cgi?id=3536

http://www.proftpd.org/docs/RELEASE_NOTES-1.3.3d

Solution

Upgrade to ProFTPD version 1.3.3d or later.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	44933
CVE	CVE-2010-4652
XREF	OSVDB:70782

Ports

tcp/21

```
 Version source    : 220 ProFTPD 1.2.5 Server (ProFTPD Default Installation)
[SECURITYFAIL.localdomain]
 Installed version : 1.2.5
 Fixed version     : 1.3.3d
```

11849 - ProFTPD File Transfer Newline Character Overflow

Synopsis

Arbitrary code may be run on the remote server.

Description

The remote host is running a version of ProFTPD which seems to be vulnerable to a buffer overflow when a user downloads a malformed ASCII file.
An attacker with upload privileges on this host may abuse this flaw to gain a root shell on this host.
*** The author of ProFTPD did not increase the version number
*** of his product when fixing this issue, so it might be false
*** positive.

Solution

Upgrade to ProFTPD 1.2.9 when available or to 1.2.8p

Risk Factor

High

CVSS Base Score

9.0 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

CVSS Temporal Score

7.4 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

References

BID	8679
CVE	CVE-2003-0831
XREF	OSVDB:10769
XREF	CWE:119

Ports

tcp/21

17718 - ProFTPD < 1.3.1rc1 mod_ctrls Module pr_ctrls_recv_request Function Local Overflow

Synopsis

The remote FTP server is affected by a local buffer overflow vulnerability.

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.
According to its banner, the version of ProFTPD installed on the remote host is earlier than 1.3.1rc1 and is affected by a local, stack-based buffer overflow. The function 'pr_ctrls_recv_request' in the file 'src/ctrls.c' belonging to the 'mod_ctrls' module does not properly handle large values in the 'reqarglen' parameter.
This error can allow a local attacker to execute arbitrary code.

See Also

http://www.securityfocus.com/archive/1/archive/1/454320/100/0/threaded

http://sourceforge.net/mailarchive/message.php?msg_id=168826

Solution

Upgrade to ProFTPD version 1.3.1rc1 or later.

Risk Factor

Medium

CVSS Base Score

6.6 (CVSS2#AV:L/AC:M/Au:S/C:C/I:C/A:C)

CVSS Temporal Score

5.5 (CVSS2#AV:L/AC:M/Au:S/C:C/I:C/A:C)

References

BID	21587

CVE	CVE-2006-6563
XREF	OSVDB:31509
XREF	EDB-ID:394
XREF	EDB-ID:3330
XREF	EDB-ID:3333

Exploitable with

Core Impact (true)

Ports

tcp/21

```
 Version source    : 220 ProFTPD 1.2.5 Server (ProFTPD Default Installation)
[SECURITYFAIL.localdomain]
 Installed version : 1.2.5
 Fixed version     : 1.3.1rc1
```

15484 - ProFTPD Login Timing Account Name Enumeration

Synopsis

The remote FTP server may disclose the list of valid usernames.

Description

The remote ProFTPd server is as old or older than 1.2.10
It is possible to determine which user names are valid on the remote host based on timing analysis attack of the login procedure.
An attacker may use this flaw to set up a list of valid usernames for a more efficient brute-force attack against the remote host.

Solution

Upgrade to a newer version.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

BID	11430
CVE	CVE-2004-1602
XREF	OSVDB:10758

Ports

tcp/21

22/tcp

17704 - OpenSSH S/KEY Authentication Account Enumeration

Synopsis

The remote host is susceptible to an information disclosure attack.

Description

When OpenSSH has S/KEY authentication enabled, it is possible to determine remotely if an account configured for S/KEY authentication exists.
Note that Nessus has not tried to exploit the issue, but rather only checked if OpenSSH is running on the remote host. As a result, it will not detect if the remote host has implemented a workaround.

See Also

http://www.nessus.org/u?87921f08

Solution

A patch currently does not exist for this issue. As a workaround, either set 'ChallengeResponseAuthentication' in the OpenSSH config to 'no' or use a version of OpenSSH without S/KEY support compiled in.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.8 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

BID	23601
CVE	CVE-2007-2243
XREF	OSVDB:34600
XREF	CWE:287

Ports

tcp/22

```
Version source    : SSH-2.0-OpenSSH_5.1p1 Debian-6ubuntu2
Installed version : 5.1p1
```

80/tcp

45004 - Apache 2.2 < 2.2.15 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities

Description

According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.15. Such versions are potentially affected by multiple vulnerabilities :
- A TLS renegotiation prefix injection attack is possible. (CVE-2009-3555)
- The 'mod_proxy_ajp' module returns the wrong status code if it encounters an error which causes the back-end server to be put into an error state. (CVE-2010-0408)
- The 'mod_isapi' attempts to unload the 'ISAPI.dll' when it encounters various error states which could leave call-backs in an undefined state. (CVE-2010-0425)
- A flaw in the core sub-request process code can lead to sensitive information from a request being handled by the wrong thread if a multi-threaded environment is used. (CVE-2010-0434)
- Added 'mod_reqtimeout' module to mitigate Slowloris attacks. (CVE-2007-6750)

See Also

http://httpd.apache.org/security/vulnerabilities_22.html

https://issues.apache.org/bugzilla/show_bug.cgi?id=48359

http://www.apache.org/dist/httpd/CHANGES_2.2.15

Solution

Upgrade to Apache version 2.2.15 or later.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	36935
BID	38491
BID	38494
BID	38580
CVE	CVE-2007-6750
CVE	CVE-2009-3555
CVE	CVE-2010-0408
CVE	CVE-2010-0425
CVE	CVE-2010-0434
XREF	OSVDB:59969
XREF	OSVDB:62674
XREF	OSVDB:62675
XREF	OSVDB:62676
XREF	IAVA:2009-A-0122
XREF	IAVA:2010-A-0041
XREF	IAVA:2010-A-0047
XREF	IAVA:2010-A-0048
XREF	IAVA:2010-A-0072
XREF	IAVA:2010-A-0089
XREF	IAVA:2010-A-0108
XREF	IAVA:2010-A-0149
XREF	IAVA:2010-A-0155
XREF	IAVA:2011-A-0007
XREF	IAVA:2011-A-0055
XREF	IAVA:2011-A-0058
XREF	IAVA:2011-A-0107
XREF	Secunia:38776
XREF	CWE:200

Exploitable with

Core Impact (true)

Ports

tcp/80

```
Version source    : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version     : 2.2.15
```

42052 - Apache 2.2 < 2.2.14 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.14. Such versions are potentially affected by multiple vulnerabilities :
- Faulty error handling in the Solaris pollset support could lead to a denial of service. (CVE-2009-2699)
- The 'mod_proxy_ftp' module allows remote attackers to bypass intended access restrictions. (CVE-2009-3095)
- The 'ap_proxy_ftp_handler' function in 'modules/proxy/proxy_ftp.c' in the 'mod_proxy_ftp' module allows remote FTP servers to cause a denial-of-service. (CVE-2009-3094)
Note that the remote web server may not actually be affected by these vulnerabilities as Nessus did not try to determine whether the affected modules are in use or check for the issues themselves.

See Also

http://www.securityfocus.com/advisories/17947

http://www.securityfocus.com/advisories/17959

http://www.intevydis.com/blog/?p=59

https://issues.apache.org/bugzilla/show_bug.cgi?id=47645

http://www.apache.org/dist/httpd/CHANGES_2.2.14

Solution

Either ensure the affected modules are not in use or upgrade to Apache version 2.2.14 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	36254
BID	36260
BID	36596
CVE	CVE-2009-2699
CVE	CVE-2009-3094
CVE	CVE-2009-3095
XREF	OSVDB:57851
XREF	OSVDB:57882
XREF	OSVDB:58879
XREF	Secunia:36549
XREF	CWE:264

Ports

tcp/80

```
Version source    : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version     : 2.2.14
```

55976 - Apache HTTP Server Byte Range DoS

Synopsis

The web server running on the remote host is affected by a denial of service vulnerability.

Description

The version of Apache HTTP Server running on the remote host is affected by a denial of service vulnerability. Making a series of HTTP requests with overlapping ranges in the Range or Request-Range request headers can result in memory and CPU exhaustion. A remote, unauthenticated attacker could exploit this to make the system unresponsive. Exploit code is publicly available and attacks have reportedly been observed in the wild.

See Also

http://archives.neohapsis.com/archives/fulldisclosure/2011-08/0203.html

http://www.gossamer-threads.com/lists/apache/dev/401638

http://www.nessus.org/u?404627ec

http://httpd.apache.org/security/CVE-2011-3192.txt

http://www.nessus.org/u?1538124a

http://www-01.ibm.com/support/docview.wss?uid=swg24030863

Solution

Upgrade to Apache httpd 2.2.21 or later, or use one of the workarounds in Apache's advisories for CVE-2011-3192. Version 2.2.20 fixed the issue, but also introduced a regression.
If the host is running a web server based on Apache httpd, contact the vendor for a fix.

Risk Factor

High

CVSS Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS Temporal Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

References

BID	49303
CVE	CVE-2011-3192
XREF	OSVDB:74721
XREF	CERT:405811
XREF	EDB-ID:17696
XREF	EDB-ID:18221
XREF	IAVA:2011-A-0120
XREF	IAVA:2011-A-0130
XREF	IAVA:2011-A-0141

Ports

tcp/80

```
Nessus determined the server is unpatched and is not using any
of the suggested workarounds by making the following requests :

-------------------- Testing for workarounds --------------------
HEAD / HTTP/1.1
Host: 192.168.150.131
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Request-Range: bytes=5-0,1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9,10-10
Range: bytes=5-0,1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9,10-10
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

HTTP/1.1 206 Partial Content
Date: Tue, 13 Mar 2012 00:38:10 GMT
Server: Apache/2.2.12 (Ubuntu)
Last-Modified: Thu, 23 Feb 2012 03:11:25 GMT
ETag: "d82-141-4b998ffda51d0"
Accept-Ranges: bytes
Content-Length: 826
Vary: Accept-Encoding
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: multipart/x-byteranges; boundary=4bb1512c58ca577c
-------------------- Testing for [...]
```

17693 - Apache mod_suexec Multiple Privilege Escalation Vulnerabilities

Synopsis

The remote Apache server is vulnerable to multiple privilege escalation attacks.

Description

The remote host appears to be running Apache and is potentially affected by the following vulnerabilities:
- Multiple race conditions exist in suexec between the validation and usage of directories and files. Under certain conditions local users are able to escalate privileges and execute arbitrary code through the renaming of directories or symlink attacks.
(CVE-2007-1741)
- Apache's suexec module only performs partial comparisons on paths, which could result in privilege escalation.
(CVE-2007-1742)
- Apache's suexec module does not properly verify user and group IDs on the command line. When the '/proc' filesystem is mounted, a local user can utilize suexec to escalate privileges. (CVE-2007-1743)

See Also

http://marc.info/?l=apache-httpd-dev&m=117511568709063&w=2

http://marc.info/?l=apache-httpd-dev&m=117511834512138&w=2

Solution

Disable suexec or disallow users from writing to the document root.

Risk Factor

Medium

CVSS Base Score

6.2 (CVSS2#AV:L/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.6 (CVSS2#AV:L/AC:H/Au:N/C:C/I:C/A:C)

References

BID	23438
CVE	CVE-2007-1741
CVE	CVE-2007-1742
CVE	CVE-2007-1743

XREF	OSVDB:34872
XREF	OSVDB:38639
XREF	OSVDB:38640

Ports

tcp/80

```
Version source    : Server: Apache/2.2.12
Installed version : 2.2.12
```

50070 - Apache 2.2 < 2.2.17 Multiple Vulnerabilities

Synopsis

The remote web server may be affected by several issues.

Description

According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.17. Such versions may be affected by several issues, including :
- Errors exist in the bundled expat library that may allow an attacker to crash the server when a buffer is over- read when parsing an XML document. (CVE-2009-3720 and CVE-2009-3560)
- An error exists in the 'apr_brigade_split_line' function in the bundled APR-util library. Carefully timed bytes in requests result in gradual memory increases leading to a denial of service. (CVE-2010-1623) Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves.

See Also

http://www.apache.org/dist/httpd/CHANGES_2.2.17

http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.17 or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

4.1 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

BID	37203
BID	36097
BID	43673
CVE	CVE-2009-3560
CVE	CVE-2009-3720
CVE	CVE-2010-1623
XREF	OSVDB:59737
XREF	OSVDB:60797
XREF	OSVDB:68327
XREF	Secunia:41701

XREF	CWE:119

Ports
tcp/80

```
Version source    : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version     : 2.2.17
```

53896 - Apache 2.2 < 2.2.18 APR apr_fnmatch DoS

Synopsis
The remote web server may be affected by a denial of service vulnerability.

Description
According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.18. Such versions are affected by a denial of service vulnerability due to an error in the 'apr_fnmatch'
match function of the bundled APR library.
If mod_autoindex is enabled and has indexed a directory containing files whose filenames are long, an attacker can cause high CPU usage with a specially crafted request.
Note that the remote web server may not actually be affected by this vulnerability. Nessus did not try to determine whether the affected module is in use or to check for the issue itself.

See Also
http://www.apache.org/dist/httpd/CHANGES_2.2.18

http://httpd.apache.org/security/vulnerabilities_22.html#2.2.18

http://securityreason.com/achievement_securityalert/98

Solution
Either ensure the 'IndexOptions' configuration option is set to 'IgnoreClient' or upgrade to Apache version 2.2.18 or later.

Risk Factor
Medium

CVSS Base Score
4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS Temporal Score
3.6 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

References
BID	47820
CVE	CVE-2011-0419
XREF	OSVDB:73388
XREF	Secunia:44574

Ports
tcp/80

```
Version source    : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version     : 2.2.18
```

57791 - Apache 2.2 < 2.2.22 Multiple Vulnerabilities

Synopsis
The remote web server may be affected by multiple vulnerabilities.

Description
According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.22. It is, therefore, potentially affected by the following vulnerabilities:

- When configured as a reverse proxy, improper use of the RewriteRule and ProxyPassMatch directives could cause the web server to proxy requests to arbitrary hosts.
This could allow a remote attacker to indirectly send requests to intranet servers.
(CVE-2011-3368, CVE-2011-4317)
- A heap-based buffer overflow exists when mod_setenvif module is enabled and both a maliciously crafted 'SetEnvIf' directive and a maliciously crafted HTTP request header are used. (CVE-2011-3607)
- A format string handling error can allow the server to be crashed via maliciously crafted cookies.
(CVE-2012-0021)
- An error exists in 'scoreboard.c' that can allow local attackers to crash the server during shutdown.
(CVE-2012-0031)
- An error exists in 'protocol.c' that can allow 'HTTPOnly' cookies to be exposed to attackers through the malicious use of either long or malformed HTTP headers. (CVE-2012-0053)
Note that Nessus did not actually test for these flaws, but instead has relied on the version in the server's banner.

See Also

http://www.apache.org/dist/httpd/CHANGES_2.2.22

http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.22 or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.1 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

BID	49957
BID	50494
BID	50802
BID	51407
BID	51705
BID	51706
CVE	CVE-2011-3368
CVE	CVE-2011-3607
CVE	CVE-2011-4317
CVE	CVE-2012-0021
CVE	CVE-2012-0031
CVE	CVE-2012-0053
XREF	IAVA:2012-A-0017
XREF	OSVDB:76079
XREF	OSVDB:76744
XREF	OSVDB:77310

XREF	OSVDB:78293
XREF	OSVDB:78555
XREF	OSVDB:78556

Ports
tcp/80

```
Version source    : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version     : 2.2.22
```

17692 - Apache mod_negotiation Multi-Line Filename Upload Vulnerabilities

Synopsis
The remote web server may be affected by one or more issues.

Description
According to its self-reported banner, the version of Apache on the remote host does not properly escape filenames in 406 responses. A remote attacker might be able to leverage this to inject arbitrary HTTP headers or conduct cross-site scripting attacks by uploading a file with a specially crafted name.
Note that the remote web server may not actually be affected by these vulnerabilities as Nessus has relied solely on the version number in the server's banner.

See Also
http://www.securityfocus.com/archive/1/486847/100/0/threaded

https://issues.apache.org/bugzilla/show_bug.cgi?id=46837

http://www.nessus.org/u?164dd6e5

Solution
Apply the workaround referenced above or upgrade to Apache 2.3.2.

Risk Factor
Medium

CVSS Base Score
4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSS Temporal Score
3.6 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References
BID	27409
CVE	CVE-2008-0455
CVE	CVE-2008-0456
XREF	OSVDB:41018
XREF	OSVDB:41019
XREF	CWE:94

Ports
tcp/80

```
Version source    : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version     : 2.3.2
```

17695 - Apache Mixed Platform AddType Directive Information Disclosure

Synopsis

The remote Apache server is vulnerable to an information disclosure attack.

Description

The remote host appears to be running Apache. When Apache runs on a Unix host with a document root on a Windows SMB share, remote, unauthenticated attackers could obtain the unprocessed contents of the directory. For example, requesting a PHP file with a trailing backslash could display the file's source instead of executing it.

See Also

http://www.nessus.org/u?d73a3dc7

Solution

Ensure that the document root is not located on a Windows SMB share.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.9 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

BID	26939
CVE	CVE-2007-6514
XREF	OSVDB:43663
XREF	CWE:200

Ports

tcp/80

```
Version source    : Server: Apache/2.2.12
Installed version : 2.2.12
```

56216 - Apache 2.2 < 2.2.21 mod_proxy_ajp DoS

Synopsis

The remote web server may be affected by a denial of service vulnerability.

Description

According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.21. It therefore is potentially affected by a denial of service vulnerability.
An error exists in the 'mod_proxy_ajp' module that can allow specially crafted HTTP requests to cause a backend server to temporarily enter an error state. This vulnerability only occurs when 'mod_proxy_ajp' is used along with 'mod_proxy_balancer'.
Note that Nessus did not actually test for the flaws but instead has relied on the version in the server's banner.

See Also

http://www.apache.org/dist/httpd/CHANGES_2.2.21

http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.21 or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.6 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

References

BID	49616
CVE	CVE-2011-3348
XREF	OSVDB:75647

Ports

tcp/80

```
Version source    : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version     : 2.2.21
```

48205 - Apache 2.2 < 2.2.16 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.16. Such versions are potentially affected by multiple vulnerabilities :
- A denial-of-service vulnerability in mod_cache and mod_dav. (CVE-2010-1452)
- An information disclosure vulnerability in mod_proxy_ajp, mod_reqtimeout, and mod_proxy_http relating to timeout conditions. Note that this issue only affects Apache on Windows, Netware, and OS/2. (CVE-2010-2068)
Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves.

See Also

http://httpd.apache.org/security/vulnerabilities_22.html

https://issues.apache.org/bugzilla/show_bug.cgi?id=49246

https://issues.apache.org/bugzilla/show_bug.cgi?id=49417

http://www.apache.org/dist/httpd/CHANGES_2.2.16

Solution

Upgrade to Apache version 2.2.16 or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.1 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

BID	40827
BID	41963
CVE	CVE-2010-1452
CVE	CVE-2010-2068
XREF	OSVDB:65654
XREF	OSVDB:66745
XREF	IAVA:2010-A-0099
XREF	Secunia:40206

Ports
tcp/80

```
Version source    : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version     : 2.2.16
```

17694 - Apache on Windows mod_alias URL Validation Canonicalization CGI Source Disclosure

Synopsis

The remote web server is affected by an information disclosure issue.

Description

The version of Apache installed on the remote Windows host can be tricked into disclosing the source of its CGI scripts because of a configuration issue. Specifically, if the CGI directory is located within the document root, then requests that alter the case of the directory name will bypass the mod_cgi cgi-script handler and be treated as requests for ordinary files.

See Also

http://www.securityfocus.com/archive/1/442882/30/0/threaded

Solution

Reconfigure Apache so that the scripts directory is located outside of the document root.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.1 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

BID	19447
CVE	CVE-2006-4110
XREF	OSVDB:27913

Ports
tcp/80

```
Version source    : Server: Apache/2.2.12
Installed version : 2.2.12
```

11644 - eZ Publish articleview.php XSS

Synopsis

The remote web server is running an application that is vulnerable to a cross-site scripting attack.

Description

The remote host is using ezPublish, a content management system.
There is a flaw in the remote ezPublish which lets an attacker perform a cross-site scripting attack. An attacker may use this flaw to steal the cookies of your legitimate users.

See Also

http://archives.neohapsis.com/archives/bugtraq/2003-05/0186.html

Solution

Upgrade to ezPublish 3

Risk Factor

Medium

CVSS Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

CVSS Temporal Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

References

BID	7616
CVE	CVE-2003-0310
XREF	OSVDB:6554

Ports

tcp/80

```
Nessus was able to verify the issue using the following URL :

  http://192.168.150.131/board/index.php/article/articleview/<img
%20src="javascript:alert(document.cookie)">
```

20088 - phpMyAdmin < 2.6.4-pl3 Multiple Vulnerabilities

Synopsis

The remote web server contains a PHP application that is prone to several flaws.

Description

The version of phpMyAdmin installed on the remote host is affected by a local file inclusion vulnerability, which can be exploited by an unauthenticated attacker to read arbitrary files, and possibly even to execute arbitrary PHP code on the affected host subject to the permissions of the web server user id.
In addition, the application fails to sanitize user-supplied input to the 'hash' parameter in the 'left.php' and 'queryframe.php' scripts as well as the 'sort_order' and 'sort_by' parameters in the 'server_databases.php' script before using it to generate dynamic HTML, which can lead to cross-site scripting attacks against the affected application.

See Also

http://www.phpmyadmin.net/home_page/security.php?issue=PMASA-2005-5

Solution

Upgrade to phpMyAdmin 2.6.4-pl3 or later.

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

4.4 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

References

BID	15169
BID	15196
CVE	CVE-2005-3300
CVE	CVE-2005-3301
XREF	OSVDB:20259
XREF	OSVDB:20260
XREF	OSVDB:20261
XREF	OSVDB:20262

Ports

tcp/80

```
***** Nessus has determined the vulnerability exists on the remote
***** host simply by looking at the version number of phpMyAdmin
***** installed there.
```

51425 - phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)

Synopsis

The remote web server hosts a PHP script that is prone to a cross- site scripting attack.

Description

The version of phpMyAdmin fails to validate BBcode tags in user input to the 'error' parameter of the 'error.php' script before using it to generate dynamic HTML.
An attacker may be able to leverage this issue to inject arbitrary HTML or script code into a user's browser to be executed within the security context of the affected site. For example, this could be used to cause a page with arbitrary text and a link to an external site to be displayed.

See Also

http://www.phpmyadmin.net/home_page/security/PMASA-2010-9.php

Solution

Upgrade to phpMyAdmin 3.4.0-beta1 or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.6 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

BID	45633
CVE	CVE-2010-4480
XREF	OSVDB:69684
XREF	EDB-ID:15699

Ports

tcp/80

```
Nessus was able to exploit the issue using the following URL :

  http://192.168.150.131/phpmyadmin/error.php?type=phpmyadmin_pmasa_2010_9.nasl&error=%5ba%40http
%3a%2f%2fwww.phpmyadmin.net%2fhome_page%2fsecurity%2fPMASA-2010-9.php%40_self]Click%20here%5b%2fa]
```

57792 - Apache HTTP Server httpOnly Cookie Information Disclosure

Synopsis

The web server running on the remote host has an information disclosure vulnerability.

Description

The version of Apache HTTP Server running on the remote host has an information disclosure vulnerability. Sending a request with HTTP headers long enough to exceed the server limit causes the web server to respond with an HTTP 400. By default, the offending HTTP header and value are displayed on the 400 error page. When used in conjunction with other attacks (e.g., cross-site scripting), this could result in the compromise of httpOnly cookies.

See Also

http://fd.the-wildcat.de/apache_e36a9cf46c.php

http://httpd.apache.org/security/vulnerabilities_22.html

http://svn.apache.org/viewvc?view=revision&revision=1235454

Solution

Upgrade to Apache version 2.2.22 or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.6 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

BID	51706
CVE	CVE-2012-0053
XREF	OSVDB:78556
XREF	EDB-ID:18442
XREF	IAVA:2012-A-0017

Ports

tcp/80

3306/tcp

17835 - MySQL < 5.0.90 / 5.1.43 / 5.5.0-m2 Multiple Buffer Overflows

Synopsis

The remote database server is affected by several buffer overflow vulnerabilities.

Description

The version of MySQL installed on the remote host is older than 5.0.90, 5.1.43 or 5.5.0-m2. Such versions use yaSSL prior to 1.9.9, that is vulnerable to multiple buffer overflows. These overflows allow a remote attacker to crash the server.

See Also

http://www.nessus.org/u?409fbf00

http://www.nessus.org/u?d46c3ad9

http://bugs.mysql.com/bug.php?id=50227

http://dev.mysql.com/doc/refman/5.1/en/news-5-1-43.html

http://dev.mysql.com/doc/refman/5.0/en/news-5-0-90.html

http://www.nessus.org/u?8426d86b

http://lists.mysql.com/commits/96697

https://isc.sans.edu//diary.html?storyid=7900

Solution

Upgrade to MySQL version 5.0.90 / 5.1.43 / 5.5.0-m2 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	37640
BID	37943
BID	37974
CVE	CVE-2009-4484
XREF	OSVDB:61956
XREF	CWE:119

Exploitable with

Core Impact (true)Metasploit (true)

Ports

tcp/3306

```
Installed version : 5.1.37-1ubuntu5.1
Fixed version     : 5.1.43
```

42900 - MySQL 5.1 < 5.1.41 Multiple Vulnerabilities

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of MySQL 5.1 installed on the remote host is earlier than 5.1.41 and thus potentially affected by the following vulnerabilities :
- An incomplete fix was provided in 5.1.24 for CVE-2008-2079, a symlink-related privilege escalation issue. (Bug #39277)
- MySQL clients linked against OpenSSL are vulnerable to man-in-the-middle attacks. (Bug #47320)
- The GeomFromWKB() function can be manipulated to cause a denial of service. (Bug #47780)
- Specially crafted SELECT statements containing sub- queries in the WHERE clause can cause the server to crash. (Bug #48291)

See Also

http://bugs.mysql.com/bug.php?id=39277

http://bugs.mysql.com/bug.php?id=47320

http://bugs.mysql.com/bug.php?id=47780

http://bugs.mysql.com/bug.php?id=48291

http://dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html

http://marc.info/?l=oss-security&m=125908080222685&w=2

http://marc.info/?l=oss-security&m=125908040022018&w=2

http://bugs.mysql.com/bug.php?id=32167

Solution

Upgrade to MySQL 5.1.41 or later.

Risk Factor

Medium

CVSS Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

CVSS Temporal Score

4.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

References

BID	37075
BID	37076
BID	37297
CVE	CVE-2008-2079
CVE	CVE-2009-4019
CVE	CVE-2009-4028
CVE	CVE-2009-4030
XREF	OSVDB:44937
XREF	OSVDB:60487
XREF	OSVDB:60488
XREF	OSVDB:60489
XREF	OSVDB:60665
XREF	Secunia:37372
XREF	CWE:264

Ports

tcp/3306

```
Installed version : 5.1.37-1ubuntu5.1
Fixed version     : 5.1.41
```

46702 - MySQL Community Server < 5.1.47 / 5.0.91 Multiple Vulnerabilities

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of MySQL Community Server installed on the remote host is earlier than 5.1.47 / 5.0.91 and thus potentially affected by the following vulnerabilities :
- The server may continue reading packets indefinitely if it receives a packet larger than the maximum size of one packet, which could allow an unauthenticated, remote attacker to consume a high level of CPU and bandwidth. (Bug #50974)
- Using an overly long table name argument to the 'COM_FIELD_LIST' command, an authenticated user can overflow a buffer and execute arbitrary code on the affected host. (Bug #53237)
- Using a specially crafted table name argument to 'COM_FIELD_LIST', an authenticated user can bypass almost all forms of checks for privileges and table- level grants. (Bug #53371)

See Also

http://bugs.mysql.com/bug.php?id=50974

http://bugs.mysql.com/bug.php?id=53237

http://bugs.mysql.com/bug.php?id=53371

http://dev.mysql.com/doc/refman/5.0/en/news-5-0-91.html

http://dev.mysql.com/doc/refman/5.1/en/news-5-1-47.html

Solution

Upgrade to MySQL Community Server 5.1.47 / 5.0.91 or later.

Risk Factor

Medium

CVSS Base Score

6.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:P)

References

BID	40100
BID	40106
BID	40109
CVE	CVE-2010-1848
CVE	CVE-2010-1849
CVE	CVE-2010-1850
XREF	OSVDB:64586
XREF	OSVDB:64587
XREF	OSVDB:64588

Exploitable with

CANVAS (true)

Ports

tcp/3306

```
Installed version : 5.1.37-1ubuntu5.1
Fixed version     : 5.1.47
```

50527 - MySQL Community Server 5.1 < 5.1.52 Multiple Vulnerabilities

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of MySQL Community Server 5.1 installed on the remote host is earlier than 5.1.52 and thus potentially affected by multiple vulnerabilities:
- An error exists in the handling of 'EXPLAIN' for a 'SELECT' statement from a derived table which can cause the server to crash. (54488)
- An error exists in the handling of 'EXPLAIN EXTENDED'
when used in some prepared statements, which can cause the server to crash. (54494)
- The server does not check the type of values assigned to items of type 'GeometryCollection'. Such assignments can cause the server to crash. (55531)

See Also

http://bugs.mysql.com/bug.php?id=54488

http://bugs.mysql.com/bug.php?id=54494

http://bugs.mysql.com/bug.php?id=55531

http://dev.mysql.com/doc/refman/5.1/en/news-5-1-52.html

Solution

Upgrade to MySQL Community Server 5.1.52 or later.

Risk Factor

Medium

CVSS Base Score

4.0 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:P)

CVSS Temporal Score

3.3 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:P)

References

BID	47871
XREF	OSVDB:68995
XREF	OSVDB:68996
XREF	OSVDB:68997
XREF	Secunia:42097

Ports

tcp/3306

```
Installed version : 5.1.37-1ubuntu5.1
Fixed version     : 5.1.52
```

48759 - MySQL Community Server < 5.1.49 Multiple Vulnerabilities

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of MySQL Community Server installed on the remote host is earlier than 5.1.49 and thus potentially affected by multiple vulnerabilities:
- DDL statements could cause the server to crash. (55039)
- Joins involving a table with a unique SET column could cause the server to crash. (54575)
- Incorrect handling of NULL arguments for IN or CASE operations involving the WITH ROLLUP modifier could cause the server to crash. (54477)
- A malformed argument to the BINLOG statement could cause the server to crash. (54393)
- Using TEMPORARY InnoDB tables with nullable columns could cause the server to crash. (54044)
- Alternate reads with two indexes on a table using the HANDLER interface could cause the server to crash. (54007)
- Using EXPLAIN with queries of the form SELECT ... UNION ... ORDER BY (SELECT ... WHERE ...) could cause the server to crash. (52711)
- LOAD DATA INFILE did not check for SQL errors sent and even if errors were already reported, it sent an OK packet. Also, an assert was sometimes raised when it should not have been relating to client-server protocol checking in debug servers. (52512)

See Also

http://bugs.mysql.com/bug.php?id=55039

http://bugs.mysql.com/bug.php?id=55475

http://bugs.mysql.com/bug.php?id=54477

http://bugs.mysql.com/bug.php?id=54393

http://bugs.mysql.com/bug.php?id=54044

http://bugs.mysql.com/bug.php?id=54007

http://bugs.mysql.com/bug.php?id=52711

http://bugs.mysql.com/bug.php?id=52512

http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html

Solution

Upgrade to MySQL Community Server 5.1.49 or later.

Risk Factor

Medium

CVSS Base Score

4.0 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:P)

CVSS Temporal Score

3.3 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:P)

References

BID	42596
BID	42598
BID	42599
BID	42625
BID	42633
BID	42638
BID	42643
BID	42646
CVE	CVE-2010-3676
CVE	CVE-2010-3677
CVE	CVE-2010-3678
CVE	CVE-2010-3679
CVE	CVE-2010-3680
CVE	CVE-2010-3681
CVE	CVE-2010-3682
CVE	CVE-2010-3683
XREF	OSVDB:67377
XREF	OSVDB:67378
XREF	OSVDB:67379
XREF	OSVDB:67380
XREF	OSVDB:67381
XREF	OSVDB:67382
XREF	OSVDB:67383
XREF	OSVDB:67384
XREF	OSVDB:69000
XREF	Secunia:41048

Ports

tcp/3306

```
Installed version : 5.1.37-1ubuntu5.1
Fixed version     : 5.1.49
```

47158 - MySQL Community Server < 5.1.48 Denial of Service

Synopsis

The remote database server is affected by denial of service vulnerability.

Description

The version of MySQL Community Server installed on the remote host is earlier than 5.1.48 and thus potentially affected by a denial of service vulnerability.
The 'ALTER DATABASE' command can be misused by a user with 'ALTER' permissions to cause the MySQL data directory to become unusable.

See Also

http://bugs.mysql.com/bug.php?id=53804

http://dev.mysql.com/doc/refman/5.1/en/news-5-1-48.html

Solution

Upgrade to MySQL Community Server 5.1.48 or later.

Risk Factor

Low

CVSS Base Score

3.5 (CVSS2#AV:N/AC:M/Au:S/C:N/I:N/A:P)

CVSS Temporal Score

2.9 (CVSS2#AV:N/AC:M/Au:S/C:N/I:N/A:P)

References

BID	41198
CVE	CVE-2010-2008
XREF	OSVDB:65851
XREF	Secunia:40333

Ports

tcp/3306

```
Installed version : 5.1.37-1ubuntu5.1
Fixed version     : 5.1.48
```

46328 - MySQL Community Server 5.1 < 5.1.46 Multiple Vulnerabilities

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of MySQL Community Server 5.1 installed on the remote host is earlier than 5.1.46 and thus potentially affected by the following vulnerabilities :
- A local user may be able to issue a 'DROP TABLE' command for one MyISAM table and remove the data and index files of a different MyISAM table. (Bug #40980)
- The application does not correct check privileges in calls to 'UNINSTALL PLUGIN', which could be abused by an unprivileged user to uninstall plugins loaded dynamically. (Bug #51770)

See Also

http://bugs.mysql.com/bug.php?id=40980

http://bugs.mysql.com/bug.php?id=51770

http://dev.mysql.com/doc/refman/5.1/en/news-5-1-46.html

Solution

Upgrade to MySQL Community Server 5.1.46 or later.

Risk Factor

Low

CVSS Base Score

3.6 (CVSS2#AV:N/AC:H/Au:S/C:N/I:P/A:P)

CVSS Temporal Score

3.0 (CVSS2#AV:N/AC:H/Au:S/C:N/I:P/A:P)

References

BID	39543
BID	40257
CVE	CVE-2010-1621
CVE	CVE-2010-1626
XREF	OSVDB:63903
XREF	OSVDB:64843

Ports

tcp/3306

```
Installed version : 5.1.37-1ubuntu5.1
Fixed version     : 5.1.46
```

17811 - MySQL < 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 Client Cross-Site Scripting

Synopsis

A remote database client have a cross-site scripting vulnerability.

Description

The version of MySQL installed on the remote host is earlier than 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 and thus does not properly encode angle brackets when 'mysql --html' option is used. Depending on how the output of the mysql client command is processed, the user may be vulnerable to cross-site scripting attacks.

See Also

http://bugs.mysql.com/bug.php?id=27884

Solution

Upgrade to MySQL version 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 or later.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

2.1 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

References

BID	31486
CVE	CVE-2008-4456
XREF	OSVDB:48710
XREF	CWE:79

Ports

tcp/3306

```
Installed version : 5.1.37-1ubuntu5.1
Fixed version     : 5.1.42
```