Nessus Report

Report

21/Mar/2012:09:07:06 GMT

Table Of Contents

Vulnerabilities By Plugin

33850 (1) - Unsupported Unix Operating System

Synopsis

The remote host is running an obsolete operating system.

Description

According to its version, the remote Unix operating system is obsolete and no longer maintained by its vendor or provider.
Lack of support implies that no new security patches will be released for it.

Solution

Upgrade to a newer version.

Risk Factor

Critical

CVSS Base Score

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

Hosts

192.168.1.10 (tcp/0)

```
Debian 5.0 support ended on 2012-02-06.
Upgrade to Debian Linux 6.0 ("Squeeze").

For more information, see : http://www.debian.org/releases/
```

55172 (1) - USN-1154-1 : openjdk-6, openjdk-6b18 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that a heap overflow in the AWT FileDialog.show() method could allow an attacker to cause a denial of service through an application crash or possibly execute arbitrary code.
(CVE-2011-0815)
It was dicovered that integer overflows in the JPEGImageReader readImage() function and the SunLayoutEngine nativeLayout() function could allow an attacker to cause a denial of service through an application crash or possibly execute arbitrary code. (CVE-2011-0822, CVE-2011-0862)
It was discovered that memory corruption could occur when interpreting bytecode in the HotSpot VM. This could allow an attacker to cause a denial of service through an application crash or possibly execute arbitrary code.
(CVE-2011-0864)
It was discovered that the deserialization code allowed the creation of mutable SignedObjects. This could allow an attacker to possibly execute code with elevated privileges. (CVE-2011-0865)
It was discovered that the toString method in the NetworkInterface class would reveal multiple addresses if they were bound to the interface. This could give an attacker more information about the networking environment.
(CVE-2011-0867)
It was discovered that the Java 2D code to transform an image with a scale close to 0 could trigger an integer overflow. This could allow an attacker to cause a denial of service through an application crash or possibly execute arbitrary code. (CVE-2011-0868)
It was discovered that the SOAP with Attachments API for Java (SAAJ) implementation allowed the modification of proxy settings via unprivileged SOAP messages. (CVE-2011-0869, CVE-2011-0870)
It was the discovered that the Swing ImageIcon class created MediaTracker objects that potentially leaked privileged ApplicationContexts. This could possibly allow an attacker access to restricted resources or services.
(CVE-2011-0871)
It was discovered that non-blocking sockets marked as not urgent could still get selected for read operations. This could allow an attacker to cause a denial of service. (CVE-2011-0872)

See Also

http://www.ubuntu.com/usn/usn-1154-1/

Solution

Update the affected package(s).

Risk Factor

Critical

CVSS Base Score

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

References

CVE	CVE-2011-0815
CVE	CVE-2011-0822
CVE	CVE-2011-0862
CVE	CVE-2011-0864
CVE	CVE-2011-0865
CVE	CVE-2011-0867
CVE	CVE-2011-0868
CVE	CVE-2011-0869
CVE	CVE-2011-0870
CVE	CVE-2011-0871

CVE	CVE-2011-0872
XREF	IAVA:2011-A-0102
XREF	IAVA:2011-A-0104
XREF	USN:1154-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : openjdk-6-jre_6b20-1.9.7-0ubuntu1~10.04.1
    Fixed package     : openjdk-6-jre_6b20-1.9.8-0ubuntu1~10.04.1

  - Installed package : openjdk-6-jre-headless_6b20-1.9.7-0ubuntu1~10.04.1
    Fixed package     : openjdk-6-jre-headless_6b20-1.9.8-0ubuntu1~10.04.1

  - Installed package : openjdk-6-jre-lib_6b20-1.9.7-0ubuntu1~10.04.1
    Fixed package     : openjdk-6-jre-lib_6b20-1.9.8-0ubuntu1~10.04.1
```

55407 (1) - USN-1149-1 : firefox, xulrunner-1.9.2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Multiple memory vulnerabilities were discovered in the browser rendering engine. An attacker could use these to possibly execute arbitrary code with the privileges of the user invoking Firefox.
(CVE-2011-2364, CVE-2011-2365, CVE-2011-2374, CVE-2011-2376)
Martin Barbella discovered that under certain conditions, viewing a XUL document while JavaScript was disabled caused deleted memory to be accessed. An attacker could potentially use this to crash Firefox or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-2373) Jordi Chancel discovered a vulnerability on multipart/x-mixed-replace images due to memory corruption. An attacker could potentially use this to crash Firefox or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-2377) Chris Rohlf and Yan Ivnitskiy discovered an integer overflow vulnerability in JavaScript Arrays. An attacker could potentially use this to execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-2371)
Multiple use-after-free vulnerabilities were discovered. An attacker could potentially use these to execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-0083, CVE-2011-0085, CVE-2011-2363)
David Chan discovered that cookies did not honor same-origin conventions. This could potentially lead to cookie data being leaked to a third party. (CVE-2011-2362)

See Also

http://www.ubuntu.com/usn/usn-1149-1/

Solution

Update the affected package(s).

Risk Factor

Critical

CVSS Base Score

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

References

CVE	CVE-2011-0083
CVE	CVE-2011-0085
CVE	CVE-2011-2362
CVE	CVE-2011-2363
CVE	CVE-2011-2364
CVE	CVE-2011-2365
CVE	CVE-2011-2371
CVE	CVE-2011-2373
CVE	CVE-2011-2374
CVE	CVE-2011-2376
CVE	CVE-2011-2377
XREF	USN:1149-1

Exploitable with

Metasploit (true)

Hosts

192.168.1.248 (tcp/0)

```
- Installed package : xulrunner-1.9.2_1.9.2.17+build3+nobinonly-0ubuntu0.10.04.1
  Fixed package     : xulrunner-1.9.2_1.9.2.18+build2+nobinonly-0ubuntu0.10.04.1
```

55921 (1) - USN-1184-1 : firefox, xulrunner-1.9.2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Gary Kwong, Igor Bukanov, and Bob Clary discovered multiple memory vulnerabilities in the browser rendering engine. An attacker could use these to possibly execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-2982)
It was discovered that a vulnerability in event management code could permit JavaScript to be run in the wrong context. This could potentially allow a malicious website to run code as another website or with escalated privileges within the browser. (CVE-2011-2981)
It was discovered that an SVG text manipulation routine contained a dangling pointer vulnerability. An attacker could potentially use this to crash Firefox or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-0084)
It was discovered that web content could receive chrome privileges if it registered for drop events and a browser tab element was dropped into the content area. This could potentially allow a malicious website to run code with escalated privileges within the browser.
(CVE-2011-2984)
It was discovered that appendChild contained a dangling pointer vulnerability. An attacker could potentially use this to crash Firefox or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-2378)
It was discovered that data from other domains could be read when RegExp.input was set. This could potentially allow a malicious website access to private data from other domains. (CVE-2011-2983)

See Also

http://www.ubuntu.com/usn/usn-1184-1/

Solution

Update the affected package(s).

Risk Factor

Critical

CVSS Base Score

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

References

CVE	CVE-2011-0084
CVE	CVE-2011-2378
CVE	CVE-2011-2981
CVE	CVE-2011-2982
CVE	CVE-2011-2983
CVE	CVE-2011-2984
XREF	USN:1184-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : xulrunner-1.9.2_1.9.2.17+build3+nobinonly-0ubuntu0.10.04.1
    Fixed package     : xulrunner-1.9.2_1.9.2.20+build1+nobinonly-0ubuntu0.10.04.1
```

56330 (1) - USN-1210-1 : firefox, xulrunner-1.9.2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Benjamin Smedberg, Bob Clary, Jesse Ruderman, and Josh Aas discovered multiple memory vulnerabilities in the browser rendering engine. An attacker could use these to possibly execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-2995, CVE-2011-2996)
Boris Zbarsky discovered that a frame named 'location' could shadow the window.location object unless a script in a page grabbed a reference to the true object before the frame was created. This is in violation of the Same Origin Policy. A malicious website could possibly use this to access another website or the local file system.
(CVE-2011-2999)
Mark Kaplan discovered an integer underflow in the SpiderMonkey JavaScript engine. An attacker could potentially use this to crash Firefox.
Ian Graham discovered that when multiple Location headers were present, Firefox would use the second one resulting in a possible CRLF injection attack. CRLF injection issues can result in a wide variety of attacks, such as XSS (Cross-Site Scripting) vulnerabilities, browser cache poisoning, and cookie theft.
(CVE-2011-3000)
Mariusz Mlynski discovered that if the user could be convinced to hold down the enter key, a malicious website could potential pop up a download dialog and the default open action would be selected. This would result in potentially malicious content being run with privileges of the user invoking Firefox. (CVE-2011-2372)

See Also

http://www.ubuntu.com/usn/usn-1210-1/

Solution

Update the affected package(s).

Risk Factor

Critical

CVSS Base Score

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

References

CVE	CVE-2011-2372
CVE	CVE-2011-2995
CVE	CVE-2011-2996
CVE	CVE-2011-2999
CVE	CVE-2011-3000
CVE	CVE-2011-3001
XREF	IAVA:2011-A-0133
XREF	USN:1210-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : xulrunner-1.9.2_1.9.2.17+build3+nobinonly-0ubuntu0.10.04.1
    Fixed package     : xulrunner-1.9.2_1.9.2.23+build1+nobinonly-0ubuntu0.10.04.1
```

56860 (1) - USN-1263-1 : icedtea-web, openjdk-6, openjdk-6b18 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Deepak Bhole discovered a flaw in the Same Origin Policy (SOP) implementation in the IcedTea web browser plugin. This could allow a remote attacker to open connections to certain hosts that should not be permitted.
(CVE-2011-3377)
Juliano Rizzo and Thai Duong discovered that the block-wise AES encryption algorithm block-wise as used in TLS/SSL was vulnerable to a chosen-plaintext attack. This could allow a remote attacker to view confidential data.
(CVE-2011-3389)
It was discovered that a type confusion flaw existed in the in the Internet Inter-Orb Protocol (IIOP) deserialization code. A remote attacker could use this to cause an untrusted application or applet to execute arbitrary code by deserializing malicious input.
(CVE-2011-3521)
It was discovered that the Java scripting engine did not perform SecurityManager checks. This could allow a remote attacker to cause an untrusted application or applet to execute arbitrary code with the full privileges of the JVM.
(CVE-2011-3544)
It was discovered that the InputStream class used a global buffer to store input bytes skipped. An attacker could possibly use this to gain access to sensitive information. (CVE-2011-3547)
It was discovered that a vulnerability existed in the AWTKeyStroke class. A remote attacker could cause an untrusted application or applet to execute arbitrary code. (CVE-2011-3548)
It was discovered that an integer overflow vulnerability existed in the TransformHelper class in the Java2D implementation. A remote attacker could use this cause a denial of service via an application or applet crash or possibly execute arbitrary code. (CVE-2011-3551)
It was discovered that the default number of available UDP sockets for applications running under SecurityManager restrictions was set too high. A remote attacker could use this with a malicious application or applet exhaust the number of available UDP sockets to cause a denial of service for other applets or applications running within the same JVM. (CVE-2011-3552)
It was discovered that Java API for XML Web Services (JAX-WS) could incorrectly expose a stack trace. A remote attacker could potentially use this to gain access to sensitive information. (CVE-2011-3553)
It was discovered that the unpacker for pack200 JAR files did not sufficiently check for errors. An attacker could cause a denial of service or possibly execute arbitrary code through a specially crafted pack200 JAR file. (CVE-2011-3554)
It was discovered that the RMI registration implementation did not properly restrict privileges of remotely executed code. A remote attacker could use this to execute code with elevated privileges.
(CVE-2011-3556, CVE-2011-3557)
It was discovered that the HotSpot VM could be made to crash, allowing an attacker to cause a denial of service or possibly leak sensitive information. (CVE-2011-3558)
It was discovered that the HttpsURLConnection class did not properly perform SecurityManager checks in certain situations. This could allow a remote attacker to bypass restrictions on HTTPS connections.
(CVE-2011-3560)

See Also

http://www.ubuntu.com/usn/usn-1263-1/

Solution

Update the affected package(s).

Risk Factor

Critical

CVSS Base Score

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

References

CVE	CVE-2011-3377
CVE	CVE-2011-3389
CVE	CVE-2011-3521
CVE	CVE-2011-3544

CVE	CVE-2011-3547
CVE	CVE-2011-3548
CVE	CVE-2011-3551
CVE	CVE-2011-3552
CVE	CVE-2011-3553
CVE	CVE-2011-3554
CVE	CVE-2011-3556
CVE	CVE-2011-3557
CVE	CVE-2011-3558
CVE	CVE-2011-3560
XREF	IAVA:2011-A-0142
XREF	IAVA:2012-A-0004
XREF	IAVA:2011-A-0155
XREF	USN:1263-1

Exploitable with

CANVAS (true)Metasploit (true)

Hosts

192.168.1.248 (tcp/0)

```
- Installed package : icedtea-6-jre-cacao_6b20-1.9.7-0ubuntu1~10.04.1
  Fixed package     : icedtea-6-jre-cacao_6b20-1.9.10-0ubuntu1~10.04.2

- Installed package : openjdk-6-jre_6b20-1.9.7-0ubuntu1~10.04.1
  Fixed package     : openjdk-6-jre_6b20-1.9.10-0ubuntu1~10.04.2

- Installed package : openjdk-6-jre-headless_6b20-1.9.7-0ubuntu1~10.04.1
  Fixed package     : openjdk-6-jre-headless_6b20-1.9.10-0ubuntu1~10.04.2

- Installed package : openjdk-6-jre-lib_6b20-1.9.7-0ubuntu1~10.04.1
  Fixed package     : openjdk-6-jre-lib_6b20-1.9.10-0ubuntu1~10.04.2
```

57436 (1) - USN-1317-1 : ghostscript vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that Ghostscript did not correctly handle memory allocation when parsing certain malformed JPEG-2000 images. If a user or automated system were tricked into opening a specially crafted image, an attacker could cause a denial of service and possibly execute arbitrary code with user privileges. (CVE-2008-3520)
It was discovered that Ghostscript did not correctly handle certain formatting operations when parsing JPEG-2000 images. If a user or automated system were tricked into opening a specially crafted image, an attacker could cause a denial of service and possibly execute arbitrary code with user privileges. (CVE-2008-3522)
It was discovered that Ghostscript incorrectly handled certain malformed TrueType fonts. If a user or automated system were tricked into opening a document containing a specially crafted font, an attacker could cause a denial of service and possibly execute arbitrary code with user privileges. This issue only affected Ubuntu 8.04 LTS. (CVE-2009-3743)
It was discovered that Ghostscript incorrectly handled certain malformed Type 2 fonts. If a user or automated system were tricked into opening a document containing a specially crafted font, an attacker could cause a denial of service and possibly execute arbitrary code with user privileges. This issue only affected Ubuntu 8.04 LTS. (CVE-2010-4054)
Jonathan Foote discovered that Ghostscript incorrectly handled certain malformed JPEG-2000 image files. If a user or automated system were tricked into opening a specially crafted JPEG-2000 image file, an attacker could cause Ghostscript to crash or possibly execute arbitrary code with user privileges. (CVE-2011-4516, CVE-2011-4517)

See Also

http://www.ubuntu.com/usn/usn-1317-1/

Solution

Update the affected package(s).

Risk Factor

Critical

CVSS Base Score

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

References

CVE	CVE-2008-3520
CVE	CVE-2008-3522
CVE	CVE-2009-3743
CVE	CVE-2010-4054
CVE	CVE-2011-4516
CVE	CVE-2011-4517
XREF	USN:1317-1
XREF	CWE:119

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libgs8_8.71.dfsg.1-0ubuntu5.3
    Fixed package     : libgs8_8.71.dfsg.1-0ubuntu5.4
```

57685 (1) - USN-1263-2 : openjdk-6, openjdk-6b18 regression

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-1263-1 fixed vulnerabilities in OpenJDK 6. The upstream patch for the chosen plaintext attack on the block-wise AES encryption algorithm (CVE-2011-3389) introduced a regression that caused TLS/SSL connections to fail when using certain algorithms. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Deepak Bhole discovered a flaw in the Same Origin Policy (SOP) implementation in the IcedTea web browser plugin. This could allow a remote attacker to open connections to certain hosts that should not be permitted.
(CVE-2011-3377) Juliano Rizzo and Thai Duong discovered that the block-wise AES encryption algorithm block-wise as used in TLS/SSL was vulnerable to a chosen-plaintext attack. This could allow a remote attacker to view confidential data. (CVE-2011-3389) It was discovered that a type confusion flaw existed in the in the Internet Inter-Orb Protocol (IIOP) deserialization code. A remote attacker could use this to cause an untrusted application or applet to execute arbitrary code by deserializing malicious input.
(CVE-2011-3521) It was discovered that the Java scripting engine did not perform SecurityManager checks. This could allow a remote attacker to cause an untrusted application or applet to execute arbitrary code with the full privileges of the JVM. (CVE-2011-3544) It was discovered that the InputStream class used a global buffer to store input bytes skipped. An attacker could possibly use this to gain access to sensitive information. (CVE-2011-3547) It was discovered that a vulnerability existed in the AWTKeyStroke class. A remote attacker could cause an untrusted application or applet to execute arbitrary code. (CVE-2011-3548) It was discovered that an integer overflow vulnerability existed in the TransformHelper class in the Java2D implementation. A remote attacker could use this cause a denial of service via an application or applet crash or possibly execute arbitrary code. (CVE-2011-3551) It was discovered that the default number of available UDP sockets for applications running under SecurityManager restrictions was set too high. A remote attacker could use this with a malicious application or applet exhaust the number of available UDP sockets to cause a denial of service for other applets or applications running within the same JVM. (CVE-2011-3552) It was discovered that Java API for XML Web Services (JAX-WS) could incorrectly expose a stack trace. A remote attacker could potentially use this to gain access to sensitive information. (CVE-2011-3553) It was discovered that the unpacker for pack200 JAR files did not sufficiently check for errors. An attacker could cause a denial of service or possibly execute arbitrary code through a specially crafted pack200 JAR file. (CVE-2011-3554) It was discovered that the RMI registration implementation did not properly restrict privileges of remotely executed code. A remote attacker could use this to execute code with elevated privileges.
(CVE-2011-3556, CVE-2011-3557) It was discovered that the HotSpot VM could be made to crash, allowing an attacker to cause a denial of service or possibly leak sensitive information. (CVE-2011-3558) It was discovered that the HttpsURLConnection class did not properly perform SecurityManager checks in certain situations. This could allow a remote attacker to bypass restrictions on HTTPS connections.
(CVE-2011-3560)

See Also

http://www.ubuntu.com/usn/usn-1263-2/

Solution

Update the affected package(s).

Risk Factor

Critical

CVSS Base Score

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

References

CVE	CVE-2011-3377
CVE	CVE-2011-3389
CVE	CVE-2011-3521
CVE	CVE-2011-3544
CVE	CVE-2011-3547

CVE	CVE-2011-3548
CVE	CVE-2011-3551
CVE	CVE-2011-3552
CVE	CVE-2011-3553
CVE	CVE-2011-3554
CVE	CVE-2011-3556
CVE	CVE-2011-3557
CVE	CVE-2011-3558
CVE	CVE-2011-3560
XREF	USN:1263-2
XREF	IAVA:2011-A-0142
XREF	IAVA:2011-A-0155
XREF	IAVA:2012-A-0004

Exploitable with

CANVAS (true)Metasploit (true)

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : icedtea-6-jre-cacao_6b20-1.9.7-0ubuntu1~10.04.1
    Fixed package     : icedtea-6-jre-cacao_6b20-1.9.10-0ubuntu1~10.04.3

  - Installed package : openjdk-6-jre_6b20-1.9.7-0ubuntu1~10.04.1
    Fixed package     : openjdk-6-jre_6b20-1.9.10-0ubuntu1~10.04.3

  - Installed package : openjdk-6-jre-headless_6b20-1.9.7-0ubuntu1~10.04.1
    Fixed package     : openjdk-6-jre-headless_6b20-1.9.10-0ubuntu1~10.04.3

  - Installed package : openjdk-6-jre-lib_6b20-1.9.7-0ubuntu1~10.04.1
    Fixed package     : openjdk-6-jre-lib_6b20-1.9.10-0ubuntu1~10.04.3
```

57844 (1) - USN-1355-1 : firefox vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that if a user chose to export their Firefox Sync key the 'Firefox Recovery Key.html' file is saved with incorrect permissions, making the file contents potentially readable by other users. (CVE-2012-0450)
Nicolas Gregoire and Aki Helin discovered that when processing a malformed embedded XSLT stylesheet, Firefox can crash due to memory corruption. If the user were tricked into opening a specially crafted page, an attacker could exploit this to cause a denial of service via application crash, or potentially execute code with the privileges of the user invoking Firefox. (CVE-2012-0449)
It was discovered that memory corruption could occur during the decoding of Ogg Vorbis files. If the user were tricked into opening a specially crafted file, an attacker could exploit this to cause a denial of service via application crash, or potentially execute code with the privileges of the user invoking Firefox. (CVE-2012-0444)
Tim Abraldes discovered that when encoding certain images types the resulting data was always a fixed size. There is the possibility of sensitive data from uninitialized memory being appended to these images. (CVE-2012-0447)
It was discovered that Firefox did not properly perform XPConnect security checks. An attacker could exploit this to conduct cross-site scripting (XSS) attacks through web pages and Firefox extensions.
With cross-site scripting vulnerabilities, if a user were tricked into viewing a specially crafted page, a remote attacker could exploit this to modify the contents, or steal confidential data, within the same domain. (CVE-2012-0446)
It was discovered that Firefox did not properly handle node removal in the DOM. If the user were tricked into opening a specially crafted page, an attacker could exploit this to cause a denial of service via application crash, or potentially execute code with the privileges of the user invoking Firefox. (CVE-2011-3659)
Alex Dvorov discovered that Firefox did not properly handle sub-frames in form submissions. An attacker could exploit this to conduct phishing attacks using HTML5 frames. (CVE-2012-0445)
Ben Hawkes, Christian Holler, Honza Bombas, Jason Orendorff, Jesse Ruderman, Jan Odvarko, Peter Van Der Beken, Bob Clary, and Bill McCloskey discovered memory safety issues affecting Firefox. If the user were tricked into opening a specially crafted page, an attacker could exploit these to cause a denial of service via application crash, or potentially execute code with the privileges of the user invoking Firefox. (CVE-2012-0442, CVE-2012-0443)

See Also

http://www.ubuntu.com/usn/usn-1355-1/

Solution

Update the affected package(s).

Risk Factor

Critical

CVSS Base Score

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

References

CVE	CVE-2011-3659
CVE	CVE-2012-0442
CVE	CVE-2012-0443
CVE	CVE-2012-0444
CVE	CVE-2012-0445
CVE	CVE-2012-0446
CVE	CVE-2012-0447
CVE	CVE-2012-0449
CVE	CVE-2012-0450
XREF	USN:1355-1

XREF	IAVA:2012-A-0018

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : firefox_9.0.1-bt0
    Fixed package     : firefox_10.0+build1-0ubuntu0.10.04.2
```

57874 (1) - USN-1353-1 : xulrunner-1.9.2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Jesse Ruderman and Bob Clary discovered memory safety issues affecting the Gecko Browser engine. If the user were tricked into opening a specially crafted page, an attacker could exploit these to cause a denial of service via application crash, or potentially execute code with the privileges of the user invoking Xulrunner.
(CVE-2012-0442)
It was discovered that the Gecko Browser engine did not properly handle node removal in the DOM. If the user were tricked into opening a specially crafted page, an attacker could exploit this to cause a denial of service via application crash, or potentially execute code with the privileges of the user invoking Xulrunner. (CVE-2011-3659)
It was discovered that memory corruption could occur during the decoding of Ogg Vorbis files. If the user were tricked into opening a specially crafted file, an attacker could exploit this to cause a denial of service via application crash, or potentially execute code with the privileges of the user invoking Xulrunner. (CVE-2012-0444)
Nicolas Gregoire and Aki Helin discovered that when processing a malformed embedded XSLT stylesheet, Xulrunner can crash due to memory corruption. If the user were tricked into opening a specially crafted page, an attacker could exploit this to cause a denial of service via application crash, or potentially execute code with the privileges of the user invoking Xulrunner. (CVE-2012-0449)
Gregory Fleischer discovered that requests using IPv6 hostname syntax through certain proxies might generate errors. An attacker might be able to use this to read sensitive data from the error messages.
(CVE-2011-3670)

See Also

http://www.ubuntu.com/usn/usn-1353-1/

Solution

Update the affected package(s).

Risk Factor

Critical

CVSS Base Score

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

References

CVE	CVE-2011-3659
CVE	CVE-2011-3670
CVE	CVE-2012-0442
CVE	CVE-2012-0444
CVE	CVE-2012-0449
XREF	USN:1353-1
XREF	IAVA:2012-A-0018

Hosts

192.168.1.248 (tcp/0)

```
- Installed package : xulrunner-1.9.2_1.9.2.17+build3+nobinonly-0ubuntu0.10.04.1
  Fixed package     : xulrunner-1.9.2_1.9.2.26+build2+nobinonly-0ubuntu0.10.04.1
```

58069 (1) - USN-1370-1 : libvorbis vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that libvorbis did not correctly handle certain malformed ogg files. If a user were tricked into opening a specially crafted ogg file with an application that uses libvorbis, an attacker could cause a denial of service or possibly execute arbitrary code with the user's privileges.

See Also

http://www.ubuntu.com/usn/usn-1370-1/

Solution

Update the affected package(s).

Risk Factor

Critical

CVSS Base Score

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

References

CVE	CVE-2012-0444
XREF	USN:1370-1
XREF	IAVA:2012-A-0018

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libvorbis0a_1.2.3-3ubuntu1
    Fixed package     : libvorbis0a_1.2.3-3ubuntu1.1
```

58130 (1) - USN-1373-1 : openjdk-6 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that the Java HttpServer class did not limit the number of headers read from a HTTP request. A remote attacker could cause a denial of service by sending special requests that trigger hash collisions predictably. (CVE-2011-5035)
ATTENTION: this update changes previous Java HttpServer class behavior by limiting the number of request headers to 200. This may be increased by adjusting the sun.net.httpserver.maxReqHeaders property.
It was discovered that the Java Sound component did not properly check buffer boundaries. A remote attacker could use this to cause a denial of service or view confidential data. (CVE-2011-3563)
It was discovered that the Java2D implementation does not properly check graphics rendering objects before passing them to the native renderer. A remote attacker could use this to cause a denial of service or to bypass Java sandbox restrictions. (CVE-2012-0497)
It was discovered that an off-by-one error exists in the Java ZIP file processing code. An attacker could us this to cause a denial of service through a maliciously crafted ZIP file. (CVE-2012-0501)
It was discovered that the Java AWT KeyboardFocusManager did not properly enforce keyboard focus security policy. A remote attacker could use this with an untrusted application or applet to grab keyboard focus and possibly expose confidential data. (CVE-2012-0502)
It was discovered that the Java TimeZone class did not properly enforce security policy around setting the default time zone. A remote attacker could use this with an untrusted application or applet to set a new default time zone and bypass Java sandbox restrictions. (CVE-2012-0503)
It was discovered the Java ObjectStreamClass did not throw an accurately identifiable exception when a deserialization failure occurred. A remote attacker could use this with an untrusted application or applet to bypass Java sandbox restrictions.
(CVE-2012-0505)
It was discovered that the Java CORBA implementation did not properly protect repository identifiers on certain CORBA objects. A remote attacker could use this to corrupt object data. (CVE-2012-0506)
It was discovered that the Java AtomicReferenceArray class implementation did not properly check if an array was of the expected Object[] type. A remote attacker could use this with a malicious application or applet to bypass Java sandbox restrictions.
(CVE-2012-0507)

See Also

http://www.ubuntu.com/usn/usn-1373-1/

Solution

Update the affected package(s).

Risk Factor

Critical

CVSS Base Score

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

References

CVE	CVE-2011-3563
CVE	CVE-2011-5035
CVE	CVE-2012-0497
CVE	CVE-2012-0501
CVE	CVE-2012-0502
CVE	CVE-2012-0503
CVE	CVE-2012-0505
CVE	CVE-2012-0506

CVE	CVE-2012-0507
XREF	USN:1373-1
XREF	IAVA:2012-A-0010
XREF	IAVA:2012-A-0028

Hosts

192.168.1.248 (tcp/0)

```
- Installed package : icedtea-6-jre-cacao_6b20-1.9.7-0ubuntu1~10.04.1
  Fixed package     : icedtea-6-jre-cacao_6b20-1.9.13-0ubuntu1~10.04.1

- Installed package : openjdk-6-jre_6b20-1.9.7-0ubuntu1~10.04.1
  Fixed package     : openjdk-6-jre_6b20-1.9.13-0ubuntu1~10.04.1

- Installed package : openjdk-6-jre-headless_6b20-1.9.7-0ubuntu1~10.04.1
  Fixed package     : openjdk-6-jre-headless_6b20-1.9.13-0ubuntu1~10.04.1

- Installed package : openjdk-6-jre-lib_6b20-1.9.7-0ubuntu1~10.04.1
  Fixed package     : openjdk-6-jre-lib_6b20-1.9.13-0ubuntu1~10.04.1
```

55168 (1) - USN-1153-1 : libxml2 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Chris Evans discovered that libxml2 incorrectly handled memory allocation. If an application using libxml2 opened a specially crafted XML file, an attacker could cause a denial of service or possibly execute code as the user invoking the program.

See Also

http://www.ubuntu.com/usn/usn-1153-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2011-1944
XREF	USN:1153-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libxml2_2.7.6.dfsg-1ubuntu1.1
    Fixed package     : libxml2_2.7.6.dfsg-1ubuntu1.2
```

55414 (1) - USN-1158-1 : curl vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Richard Silverman discovered that when doing GSSAPI authentication, libcurl unconditionally performs credential delegation, handing the server a copy of the client's security credential. (CVE-2011-2192)
Wesley Miaw discovered that when zlib is enabled, libcurl does not properly restrict the amount of callback data sent to an application that requests automatic decompression. This might allow an attacker to cause a denial of service via an application crash or possibly execute arbitrary code with the privilege of the application. This issue only affected Ubuntu 8.04 LTS and Ubuntu 10.04 LTS.
(CVE-2010-0734)
USN 818-1 fixed an issue with curl's handling of SSL certificates with zero bytes in the Common Name. Due to a packaging error, the fix for this issue was not being applied during the build. This issue only affected Ubuntu 8.04 LTS. We apologize for the error.
(CVE-2009-2417)
Original advisory details:
Scott Cantor discovered that curl did not correctly handle SSL certificates with zero bytes in the Common Name. A remote attacker could exploit this to perform a man in the middle attack to view sensitive information or alter encrypted communications.

See Also

http://www.ubuntu.com/usn/usn-1158-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2009-2417
CVE	CVE-2010-0734
CVE	CVE-2011-2192
XREF	USN:1158-1
XREF	CWE:310

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libcurl3_7.19.7-1ubuntu1
    Fixed package     : libcurl3_7.19.7-1ubuntu1.1

  - Installed package : libcurl3-gnutls_7.19.7-1ubuntu1
    Fixed package     : libcurl3-gnutls_7.19.7-1ubuntu1.1
```

55858 (1) - USN-1191-1 : libxfont vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Tomas Hoger discovered that libXfont incorrectly handled certain malformed compressed fonts. An attacker could use a specially crafted font file to cause libXfont to crash, or possibly execute arbitrary code in order to gain privileges.

See Also

http://www.ubuntu.com/usn/usn-1191-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2011-2895
XREF	USN:1191-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libxfont1_1:1.4.1-1
    Fixed package     : libxfont1_1:1.4.1-1ubuntu0.1
```

55976 (1) - Apache HTTP Server Byte Range DoS

Synopsis

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

Description

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

See Also

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

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

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

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

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

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

Solution

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

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

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

Hosts

192.168.1.248 (tcp/80)

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

-------------------- Testing for workarounds --------------------
```

```
HEAD / HTTP/1.1
Host: 192.168.1.248
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Request-Range: bytes=5-0,1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9,10-10
Range: bytes=5-0,1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9,10-10
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

HTTP/1.1 206 Partial Content
Date: Wed, 21 Mar 2012 12:27:22 GMT
Server: Apache/2.2.14 (Ubuntu)
Last-Modified: Tue, 10 May 2011 07:45:00 GMT
ETag: "493a0-b1-4a2e722183700"
Accept-Ranges: bytes
Content-Length: 826
Vary: Accept-Encoding
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: multipart/x-byteranges; boundary=4bbbfe9d305c1ddd
-------------------- Testing for  [...]
```

56036 (1) - USN-1197-1 : firefox, xulrunner-1.9.2 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that Dutch Certificate Authority DigiNotar, had mis-issued multiple fraudulent certificates. These certificates could allow an attacker to perform a 'man in the middle' (MITM) attack which would make the user believe their connection is secure, but is actually being monitored.
For the protection of its users, Mozilla has removed the DigiNotar certificate. Sites using certificates issued by DigiNotar will need to seek another certificate vendor.
We are currently aware of a regression that blocks one of two Staat der Nederlanden root certificates which are believed to still be secure. This regression is being tracked at https://launchpad.net/bugs/838322.

See Also

http://www.ubuntu.com/usn/usn-1197-1/

Solution

Update the affected package(s).

Risk Factor

High

References

XREF	USN:1197-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : xulrunner-1.9.2_1.9.2.17+build3+nobinonly-0ubuntu0.10.04.1
    Fixed package     : xulrunner-1.9.2_1.9.2.21+build1+nobinonly-0ubuntu0.10.04.1
```

56115 (1) - USN-1197-3 : firefox, xulrunner-1.9.2 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-1197-1 partially addressed an issue with Dutch Certificate Authority DigiNotar mis-issuing fraudulent certificates. This update actively distrusts the DigiNotar root certificate as well as several intermediary certificates. Also included in this list of distrusted certificates are the Staat der Nederlanden root certificates.
Original advisory details:
It was discovered that Dutch Certificate Authority DigiNotar, had mis-issued multiple fraudulent certificates. These certificates could allow an attacker to perform a 'man in the middle' (MITM) attack which would make the user believe their connection is secure, but is actually being monitored.
For the protection of its users, Mozilla has removed the DigiNotar certificate. Sites using certificates issued by DigiNotar will need to seek another certificate vendor.
We are currently aware of a regression that blocks one of two Staat der Nederlanden root certificates which are believed to still be secure. This regression is being tracked at https://launchpad.net/bugs/838322.

See Also

http://www.ubuntu.com/usn/usn-1197-3/

Solution

Update the affected package(s).

Risk Factor

High

References

XREF	USN:1197-3

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : xulrunner-1.9.2_1.9.2.17+build3+nobinonly-0ubuntu0.10.04.1
    Fixed package     : xulrunner-1.9.2_1.9.2.22+build2+nobinonly-0ubuntu0.10.04.1
```

56139 (1) - USN-1197-4 : nss vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-1197-1 and USN-1197-3 addressed an issue in Firefox and Xulrunner pertaining to the Dutch Certificate Authority DigiNotar mis-issuing fraudulent certificates. This update provides the corresponding update for the Network Security Service libraries (NSS).
Original advisory details: USN-1197-1
It was discovered that Dutch Certificate Authority DigiNotar, had mis-issued multiple fraudulent certificates. These certificates could allow an attacker to perform a 'man in the middle' (MITM) attack which would make the user believe their connection is secure, but is actually being monitored.
For the protection of its users, Mozilla has removed the DigiNotar certificate. Sites using certificates issued by DigiNotar will need to seek another certificate vendor.
We are currently aware of a regression that blocks one of two Staat der Nederlanden root certificates which are believed to still be secure. This regression is being tracked at https://launchpad.net/bugs/838322.
USN-1197-3
USN-1197-1 partially addressed an issue with Dutch Certificate Authority DigiNotar mis-issuing fraudulent certificates. This update actively distrusts the DigiNotar root certificate as well as several intermediary certificates. Also included in this list of distrusted certificates are the 'PKIOverheid' (PKIGovernment) intermediates under DigiNotar's control that did not chain to DigiNotar's root and were not previously blocked.

See Also

http://www.ubuntu.com/usn/usn-1197-4/

Solution

Update the affected package(s).

Risk Factor

High

References

XREF	USN:1197-4

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libnss3-1d_3.12.9+ckbi-1.82-0ubuntu0.10.04.1
    Fixed package     : libnss3-1d_3.12.9+ckbi-1.82-0ubuntu0.10.04.3
```

56140 (1) - USN-1197-5 : ca-certificates vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-1197-1 addressed an issue in Firefox and Xulrunner pertaining to the Dutch Certificate Authority DigiNotar mis-issuing fraudulent certificates. This update provides the corresponding update for ca-certificates.
Original advisory details:
It was discovered that Dutch Certificate Authority DigiNotar, had mis-issued multiple fraudulent certificates. These certificates could allow an attacker to perform a 'man in the middle' (MITM) attack which would make the user believe their connection is secure, but is actually being monitored.
For the protection of its users, Mozilla has removed the DigiNotar certificate. Sites using certificates issued by DigiNotar will need to seek another certificate vendor.
We are currently aware of a regression that blocks one of two Staat der Nederlanden root certificates which are believed to still be secure. This regression is being tracked at https://launchpad.net/bugs/838322.

See Also

http://www.ubuntu.com/usn/usn-1197-5/

Solution

Update the affected package(s).

Risk Factor

High

References

XREF	USN:1197-5

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : ca-certificates_20090814
    Fixed package     : ca-certificates_20090814ubuntu0.10.04.1
```

56194 (1) - USN-1206-1 : librsvg vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Sauli Pahlman discovered that librsvg did not correctly handle malformed filter names. If a user or automated system were tricked into processing a specially crafted SVG image, a remote attacker could gain user privileges.

See Also

http://www.ubuntu.com/usn/usn-1206-1/

Solution

Update the affected package(s).

Risk Factor

High

References

CVE	CVE-2011-3146
XREF	USN:1206-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : librsvg2-2_2.26.3-0ubuntu1
    Fixed package     : librsvg2-2_2.26.3-0ubuntu1.1

  - Installed package : librsvg2-common_2.26.3-0ubuntu1
    Fixed package     : librsvg2-common_2.26.3-0ubuntu1.1
```

56236 (1) - USN-1209-1 : ffmpeg vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that FFmpeg incorrectly handled certain malformed ogg files. If a user were tricked into opening a crafted ogg file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. This issue only affected Ubuntu 10.10.
(CVE-2011-1196)
It was discovered that FFmpeg incorrectly handled certain malformed AMV files. If a user were tricked into opening a crafted AMV file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. This issue only affected Ubuntu 10.10.
(CVE-2011-1931)
It was discovered that FFmpeg incorrectly handled certain malformed APE files. If a user were tricked into opening a crafted APE file, an attacker could cause a denial of service via application crash.
(CVE-2011-2161)
Emmanouel Kellinis discovered that FFmpeg incorrectly handled certain malformed CAVS files. If a user were tricked into opening a crafted CAVS file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-3362)

See Also

http://www.ubuntu.com/usn/usn-1209-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2011-1196
CVE	CVE-2011-1931
CVE	CVE-2011-2161
CVE	CVE-2011-3362
XREF	USN:1209-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libavcodec52_4:0.5.1-1ubuntu1.1
    Fixed package     : libavcodec52_4:0.5.1-1ubuntu1.2

  - Installed package : libavformat52_4:0.5.1-1ubuntu1.1
    Fixed package     : libavformat52_4:0.5.1-1ubuntu1.2
```

56281 (1) - USN-1215-1 : apt vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that the apt-key utility incorrectly verified GPG keys when downloaded via the net-update option. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could potentially be used to install altered packages. This update corrects the issue by disabling the net-update option completely. A future update will re-enable the option with corrected verification.

See Also

http://www.ubuntu.com/usn/usn-1215-1/

Solution

Update the affected package(s).

Risk Factor

High

References

XREF	USN:1215-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : apt_0.7.25.3ubuntu9.4
    Fixed package     : apt_0.7.25.3ubuntu9.7
```

56554 (1) - USN-1231-1 : php5 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Mateusz Kocielski, Marek Kroemeke and Filip Palian discovered that a stack-based buffer overflow existed in the socket_connect function's handling of long pathnames for AF_UNIX sockets. A remote attacker might be able to exploit this to execute arbitrary code; however, the default compiler options for affected releases should reduce the vulnerability to a denial of service. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04.
(CVE-2011-1938)
Krzysztof Kotowicz discovered that the PHP post handler function does not properly restrict filenames in multipart/form-data POST requests.
This may allow remote attackers to conduct absolute path traversal attacks and possibly create or overwrite arbitrary files. This issue affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-2202)
It was discovered that the crypt function for blowfish does not properly handle 8-bit characters. This could make it easier for an attacker to discover a cleartext password containing an 8-bit character that has a matching blowfish crypt value. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04.
(CVE-2011-2483)
It was discovered that PHP did not properly check the return values of the malloc(3), calloc(3) and realloc(3) library functions in multiple locations. This could allow an attacker to cause a denial of service via a NULL pointer dereference or possibly execute arbitrary code. This issue affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-3182)
Maksymilian Arciemowicz discovered that PHP did not properly implement the error_log function. This could allow an attacker to cause a denial of service via an application crash. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, Ubuntu 11.04 and Ubuntu 11.10. (CVE-2011-3267)
Maksymilian Arciemowicz discovered that the ZipArchive functions addGlob() and addPattern() did not properly check their flag arguments. This could allow a malicious script author to cause a denial of service via application crash. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, Ubuntu 11.04 and Ubuntu 11.10.
(CVE-2011-1657)
It was discovered that the Xend opcode parser in PHP could be interrupted while handling the shift-left, shift-right, and bitwise-xor opcodes. This could allow a malicious script author to expose memory contents. This issue affected Ubuntu 10.04 LTS.
(CVE-2010-1914)
It was discovered that the strrchr function in PHP could be interrupted by a malicious script, allowing the exposure of memory contents. This issue affected Ubuntu 8.04 LTS. (CVE-2010-2484)

See Also

http://www.ubuntu.com/usn/usn-1231-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2010-1914
CVE	CVE-2010-2484
CVE	CVE-2011-1657
CVE	CVE-2011-1938
CVE	CVE-2011-2202
CVE	CVE-2011-2483
CVE	CVE-2011-3182

CVE	CVE-2011-3267
XREF	USN:1231-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libapache2-mod-php5_5.3.2-1ubuntu4.9
    Fixed package     : libapache2-mod-php5_5.3.2-1ubuntu4.10

  - Installed package : php5-cli_5.3.2-1ubuntu4.9
    Fixed package     : php5-cli_5.3.2-1ubuntu4.10

  - Installed package : php5-common_5.3.2-1ubuntu4.9
    Fixed package     : php5-common_5.3.2-1ubuntu4.10
```

56555 (1) - USN-1232-1 : xorg-server vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that the X server incorrectly handled certain malformed input. An authorized attacker could exploit this to cause the X server to crash, leading to a denial or service, or possibly execute arbitrary code with root privileges. This issue only affected Ubuntu 10.04 LTS and 10.10. (CVE-2010-4818)
It was discovered that the X server incorrectly handled certain malformed input. An authorized attacker could exploit this to cause the X server to crash, leading to a denial or service, or possibly read arbitrary data from the X server process. This issue only affected Ubuntu 10.04 LTS. (CVE-2010-4819)
Vladz discovered that the X server incorrectly handled lock files. A local attacker could use this flaw to determine if a file existed or not. (CVE-2011-4028)
Vladz discovered that the X server incorrectly handled setting lock file permissions. A local attacker could use this flaw to gain read permissions on arbitrary files and view sensitive information.
(CVE-2011-4029)

See Also

http://www.ubuntu.com/usn/usn-1232-1/

Solution

Update the affected package(s).

Risk Factor

High

References

CVE	CVE-2010-4818
CVE	CVE-2010-4819
CVE	CVE-2011-4028
CVE	CVE-2011-4029
XREF	USN:1232-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : xserver-xorg-core_2:1.7.6-2ubuntu7.6
    Fixed package     : xserver-xorg-core_2:1.7.6-2ubuntu7.8
```

56563 (1) - USN-1232-2 : xorg-server regression

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-1232-1 fixed vulnerabilities in the X.Org X server. A regression was found on Ubuntu 10.04 LTS that affected GLX support.
This update temporarily disables the fix for CVE-2010-4818 that introduced the regression.
We apologize for the inconvenience.
Original advisory details:
It was discovered that the X server incorrectly handled certain malformed input. An authorized attacker could exploit this to cause the X server to crash, leading to a denial or service, or possibly execute arbitrary code with root privileges. This issue only affected Ubuntu 10.04 LTS and 10.10. (CVE-2010-4818) It was discovered that the X server incorrectly handled certain malformed input. An authorized attacker could exploit this to cause the X server to crash, leading to a denial or service, or possibly read arbitrary data from the X server process. This issue only affected Ubuntu 10.04 LTS. (CVE-2010-4819) Vladz discovered that the X server incorrectly handled lock files. A local attacker could use this flaw to determine if a file existed or not. (CVE-2011-4028) Vladz discovered that the X server incorrectly handled setting lock file permissions. A local attacker could use this flaw to gain read permissions on arbitrary files and view sensitive information.
(CVE-2011-4029)

See Also

http://www.ubuntu.com/usn/usn-1232-2/

Solution

Update the affected package(s).

Risk Factor

High

References

CVE	CVE-2010-4818
CVE	CVE-2010-4819
CVE	CVE-2011-4028
CVE	CVE-2011-4029
XREF	USN:1232-2

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : xserver-xorg-core_2:1.7.6-2ubuntu7.6
    Fixed package     : xserver-xorg-core_2:1.7.6-2ubuntu7.9
```

56580 (1) - USN-1232-3 : xorg-server vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-1232-1 fixed vulnerabilities in the X.Org X server. A regression was found on Ubuntu 10.04 LTS that affected GLX support, and USN-1232-2 was released to temporarily disable the problematic security fix. This update includes a revised fix for CVE-2010-4818.
We apologize for the inconvenience.
Original advisory details:
It was discovered that the X server incorrectly handled certain malformed input. An authorized attacker could exploit this to cause the X server to crash, leading to a denial or service, or possibly execute arbitrary code with root privileges. This issue only affected Ubuntu 10.04 LTS and 10.10. (CVE-2010-4818) It was discovered that the X server incorrectly handled certain malformed input. An authorized attacker could exploit this to cause the X server to crash, leading to a denial or service, or possibly read arbitrary data from the X server process. This issue only affected Ubuntu 10.04 LTS. (CVE-2010-4819) Vladz discovered that the X server incorrectly handled lock files. A local attacker could use this flaw to determine if a file existed or not. (CVE-2011-4028) Vladz discovered that the X server incorrectly handled setting lock file permissions. A local attacker could use this flaw to gain read permissions on arbitrary files and view sensitive information.
(CVE-2011-4029)

See Also

http://www.ubuntu.com/usn/usn-1232-3/

Solution

Update the affected package(s).

Risk Factor

High

References

CVE	CVE-2010-4818
CVE	CVE-2010-4819
CVE	CVE-2011-4028
CVE	CVE-2011-4029
XREF	USN:1232-3

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : xserver-xorg-core_2:1.7.6-2ubuntu7.6
    Fixed package     : xserver-xorg-core_2:1.7.6-2ubuntu7.10
```

56629 (1) - USN-1237-1 : pam vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Kees Cook discovered that the PAM pam_env module incorrectly handled certain malformed environment files. A local attacker could use this flaw to cause a denial of service, or possibly gain privileges. The default compiler options for affected releases should reduce the vulnerability to a denial of service. (CVE-2011-3148)
Kees Cook discovered that the PAM pam_env module incorrectly handled variable expansion. A local attacker could use this flaw to cause a denial of service. (CVE-2011-3149)
Stephane Chazelas discovered that the PAM pam_motd module incorrectly cleaned the environment during execution of the motd scripts. In certain environments, a local attacker could use this to execute arbitrary code as root, and gain privileges.

See Also

http://www.ubuntu.com/usn/usn-1237-1/

Solution

Update the affected package(s).

Risk Factor

High

References

CVE	CVE-2011-3148
CVE	CVE-2011-3149
CVE	CVE-2011-3628
XREF	USN:1237-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libpam-modules_1.1.1-2ubuntu5.1
    Fixed package     : libpam-modules_1.1.1-2ubuntu5.4
```

56767 (1) - USN-1255-1 : libmodplug vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Hossein Lotfi discovered that libmodplug did not correctly handle certain malformed media files. If a user or automated system were tricked into opening a crafted media file, an attacker could cause a denial of service or possibly execute arbitrary code with privileges of the user invoking the program. (CVE-2011-2911, CVE-2011-2912, CVE-2011-2913)
It was discovered that libmodplug did not correctly handle certain malformed media files. If a user or automated system were tricked into opening a crafted media file, an attacker could cause a denial of service or possibly execute arbitrary code with privileges of the user invoking the program. (CVE-2011-2914, CVE-2011-2915)

See Also

http://www.ubuntu.com/usn/usn-1255-1/

Solution

Update the affected package(s).

Risk Factor

High

References

CVE	CVE-2011-2911
CVE	CVE-2011-2912
CVE	CVE-2011-2913
CVE	CVE-2011-2914
CVE	CVE-2011-2915
XREF	USN:1255-1

Hosts

192.168.1.248 (tcp/0)

```
- Installed package : libmodplug0c2_1:0.8.7-1build1
  Fixed package     : libmodplug0c2_1:0.8.7-1ubuntu0.3
```

56775 (1) - USN-1251-1 : firefox, xulrunner-1.9.2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that CVE-2011-3004, which addressed possible privilege escalation in addons, also affected Firefox 3.6. An attacker could potentially exploit Firefox when an add-on was installed that used loadSubscript in vulnerable ways. (CVE-2011-3647)
Yosuke Hasegawa discovered that the Mozilla browser engine mishandled invalid sequences in the Shift-JIS encoding. A malicious website could possibly use this flaw this to steal data or inject malicious scripts into web content. (CVE-2011-3648)
Marc Schoenefeld discovered that using Firebug to profile a JavaScript file with many functions would cause Firefox to crash. An attacker might be able to exploit this without using the debugging APIs which would potentially allow an attacker to remotely crash the browser. (CVE-2011-3650)

See Also

http://www.ubuntu.com/usn/usn-1251-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2011-3004
CVE	CVE-2011-3647
CVE	CVE-2011-3648
CVE	CVE-2011-3650
XREF	IAVA:2011-A-0133
XREF	IAVA:2011-A-0154
XREF	USN:1251-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : xulrunner-1.9.2_1.9.2.17+build3+nobinonly-0ubuntu0.10.04.1
    Fixed package     : xulrunner-1.9.2_1.9.2.24+build2+nobinonly-0ubuntu0.10.04.1
```

56870 (1) - USN-1267-1 : freetype vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that FreeType did not correctly handle certain malformed Type 1 font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges.
(CVE-2011-3256)
It was discovered that FreeType did not correctly handle certain malformed CID-keyed PostScript font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges. (CVE-2011-3439)

See Also

http://www.ubuntu.com/usn/usn-1267-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2011-3256
CVE	CVE-2011-3439
XREF	USN:1267-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libfreetype6_2.3.11-1ubuntu2.4
    Fixed package     : libfreetype6_2.3.11-1ubuntu2.5
```

56970 (1) - USN-1283-1 : apt vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that APT incorrectly handled the Verify-Host configuration option. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could potentially be used to steal repository credentials. This issue only affected Ubuntu 10.04 LTS and 10.10. (CVE-2011-3634)
USN-1215-1 fixed a vulnerability in APT by disabling the apt-key net-update option. This update re-enables the option with corrected verification. Original advisory details: It was discovered that the apt-key utility incorrectly verified GPG keys when downloaded via the net-update option. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could potentially be used to install altered packages.

See Also

http://www.ubuntu.com/usn/usn-1283-1/

Solution

Update the affected package(s).

Risk Factor

High

References

CVE	CVE-2011-3634
XREF	USN:1283-1

Hosts

192.168.1.248 (tcp/0)

```
- Installed package : apt_0.7.25.3ubuntu9.4
  Fixed package     : apt_0.7.25.3ubuntu9.9
```

57315 (1) - USN-1308-1 : bzip2 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

vladz discovered that executables compressed by bzexe insecurely create temporary files when they are ran. A local attacker could exploit this issue to execute arbitrary code as the user running a compressed executable.

See Also

http://www.ubuntu.com/usn/usn-1308-1/

Solution

Update the affected package(s).

Risk Factor

High

References

CVE	CVE-2011-4089
XREF	USN:1308-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : bzip2_1.0.5-4ubuntu0.1
    Fixed package     : bzip2_1.0.5-4ubuntu0.2
```

57341 (1) - USN-1310-1 : libarchive vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that libarchive incorrectly handled certain ISO 9660 image files. If a user were tricked into using a specially crafted ISO 9660 image file, a remote attacker could cause libarchive to crash or possibly execute arbitrary code with user privileges.
(CVE-2011-1777)
It was discovered that libarchive incorrectly handled certain tar archive files. If a user were tricked into using a specially crafted tar file, a remote attacker could cause libarchive to crash or possibly execute arbitrary code with user privileges. (CVE-2011-1778)

See Also

http://www.ubuntu.com/usn/usn-1310-1/

Solution

Update the affected package(s).

Risk Factor

High

References

CVE	CVE-2011-1777
CVE	CVE-2011-1778
XREF	USN:1310-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libarchive1_2.8.0-2
    Fixed package     : libarchive1_2.8.0-2ubuntu0.1
```

57449 (1) - USN-1320-1 : ffmpeg vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Steve Manzuik discovered that FFmpeg incorrectly handled certain malformed Matroska files. If a user were tricked into opening a crafted Matroska file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-3504)
Phillip Langlois discovered that FFmpeg incorrectly handled certain malformed QDM2 streams. If a user were tricked into opening a crafted QDM2 stream file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-4351)
Phillip Langlois discovered that FFmpeg incorrectly handled certain malformed VP3 streams. If a user were tricked into opening a crafted file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. This issue only affected Ubuntu 10.10. (CVE-2011-4352)
Phillip Langlois discovered that FFmpeg incorrectly handled certain malformed VP5 and VP6 streams. If a user were tricked into opening a crafted file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-4353)
It was discovered that FFmpeg incorrectly handled certain malformed VMD files. If a user were tricked into opening a crafted VMD file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-4364)
Phillip Langlois discovered that FFmpeg incorrectly handled certain malformed SVQ1 streams. If a user were tricked into opening a crafted SVQ1 stream file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-4579)

See Also

http://www.ubuntu.com/usn/usn-1320-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2011-3504
CVE	CVE-2011-4351
CVE	CVE-2011-4352
CVE	CVE-2011-4353
CVE	CVE-2011-4364
CVE	CVE-2011-4579
XREF	USN:1320-1

Hosts

192.168.1.248 (tcp/0)

```
- Installed package : libavcodec52_4:0.5.1-1ubuntu1.1
  Fixed package     : libavcodec52_4:0.5.1-1ubuntu1.3

- Installed package : libavformat52_4:0.5.1-1ubuntu1.1
  Fixed package     : libavformat52_4:0.5.1-1ubuntu1.3
```

57615 (1) - USN-1334-1 : libxml2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that libxml2 contained an off by one error. If a user or application linked against libxml2 were tricked into opening a specially crafted XML file, an attacker could cause the application to crash or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-0216)
It was discovered that libxml2 is vulnerable to double-free conditions when parsing certain XML documents. This could allow a remote attacker to cause a denial of service. (CVE-2011-2821, CVE-2011-2834)
It was discovered that libxml2 did not properly detect end of file when parsing certain XML documents. An attacker could exploit this to crash applications linked against libxml2. (CVE-2011-3905)
It was discovered that libxml2 did not properly decode entity references with long names. If a user or application linked against libxml2 were tricked into opening a specially crafted XML file, an attacker could cause the application to crash or possibly execute arbitrary code with the privileges of the user invoking the program.
(CVE-2011-3919)

See Also

http://www.ubuntu.com/usn/usn-1334-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2011-0216
CVE	CVE-2011-2821
CVE	CVE-2011-2834
CVE	CVE-2011-3905
CVE	CVE-2011-3919
XREF	USN:1334-1

Hosts

192.168.1.248 (tcp/0)

```
- Installed package : libxml2_2.7.6.dfsg-1ubuntu1.1
  Fixed package     : libxml2_2.7.6.dfsg-1ubuntu1.3
```

57616 (1) - USN-1335-1 : t1lib vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Jon Larimer discovered that t1lib did not properly parse AFM fonts.
If a user were tricked into using a specially crafted font file, a remote attacker could cause t1lib to crash or possibly execute arbitrary code with user privileges. (CVE-2010-2642, CVE-2011-0433)
Jonathan Brossard discovered that t1lib did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause t1lib to crash. (CVE-2011-1552, CVE-2011-1553, CVE-2011-1554)

See Also

http://www.ubuntu.com/usn/usn-1335-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2010-2642
CVE	CVE-2011-0433
CVE	CVE-2011-1552
CVE	CVE-2011-1553
CVE	CVE-2011-1554
XREF	USN:1335-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libt1-5_5.1.2-3build1
    Fixed package     : libt1-5_5.1.2-3ubuntu0.10.04.2
```

57706 (1) - USN-1348-1 : icu vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that ICU did not properly handle invalid locale data during Unicode conversion. If an application using ICU processed crafted data, an attacker could cause it to crash or potentially execute arbitrary code with the privileges of the user invoking the program.

See Also

http://www.ubuntu.com/usn/usn-1348-1/

Solution

Update the affected package(s).

Risk Factor

High

References

CVE	CVE-2011-4599
XREF	USN:1348-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libicu42_4.2.1-3
    Fixed package     : libicu42_4.2.1-3ubuntu0.10.04.1
```

57707 (1) - USN-1349-1 : xorg vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that the X wrapper incorrectly checked certain console permissions when launched by unprivileged users. An attacker connected remotely could use this flaw to start X, bypassing the console permissions check.

See Also

http://www.ubuntu.com/usn/usn-1349-1/

Solution

Update the affected package(s).

Risk Factor

High

References

CVE	CVE-2011-4613
XREF	USN:1349-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : xserver-xorg_1:7.5+5ubuntu1
    Fixed package     : xserver-xorg_1:7.5+5ubuntu1.1
```

57887 (1) - USN-1357-1 : openssl vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that the elliptic curve cryptography (ECC) subsystem in OpenSSL, when using the Elliptic Curve Digital Signature Algorithm (ECDSA) for the ECDHE_ECDSA cipher suite, did not properly implement curves over binary fields. This could allow an attacker to determine private keys via a timing attack. This issue only affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04.
(CVE-2011-1945)
Adam Langley discovered that the ephemeral Elliptic Curve Diffie-Hellman (ECDH) functionality in OpenSSL did not ensure thread safety while processing handshake messages from clients. This could allow a remote attacker to cause a denial of service via out-of-order messages that violate the TLS protocol. This issue only affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04.
(CVE-2011-3210)
Nadhem Alfardan and Kenny Paterson discovered that the Datagram Transport Layer Security (DTLS) implementation in OpenSSL performed a MAC check only if certain padding is valid. This could allow a remote attacker to recover plaintext. (CVE-2011-4108)
Antonio Martin discovered that a flaw existed in the fix to address CVE-2011-4108, the DTLS MAC check failure. This could allow a remote attacker to cause a denial of service. (CVE-2012-0050)
Ben Laurie discovered a double free vulnerability in OpenSSL that could be triggered when the X509_V_FLAG_POLICY_CHECK flag is enabled.
This could allow a remote attacker to cause a denial of service. This issue only affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-4109)
It was discovered that OpenSSL, in certain circumstances involving ECDH or ECDHE cipher suites, used an incorrect modular reduction algorithm in its implementation of the P-256 and P-384 NIST elliptic curves. This could allow a remote attacker to obtain the private key of a TLS server via multiple handshake attempts. This issue only affected Ubuntu 8.04 LTS. (CVE-2011-4354)
Adam Langley discovered that the SSL 3.0 implementation in OpenSSL did not properly initialize data structures for block cipher padding.
This could allow a remote attacker to obtain sensitive information.
(CVE-2011-4576)
Andrew Chi discovered that OpenSSL, when RFC 3779 support is enabled, could trigger an assert when handling an X.509 certificate containing certificate-extension data associated with IP address blocks or Autonomous System (AS) identifiers. This could allow a remote attacker to cause a denial of service. (CVE-2011-4577)
Adam Langley discovered that the Server Gated Cryptography (SGC) implementation in OpenSSL did not properly handle handshake restarts.
This could allow a remote attacker to cause a denial of service.
(CVE-2011-4619)
Andrey Kulikov discovered that the GOST block cipher engine in OpenSSL did not properly handle invalid parameters. This could allow a remote attacker to cause a denial of service via crafted data from a TLS client. This issue only affected Ubuntu 11.10. (CVE-2012-0027)

See Also

http://www.ubuntu.com/usn/usn-1357-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2011-1945
CVE	CVE-2011-3210
CVE	CVE-2011-4108
CVE	CVE-2011-4109

CVE	CVE-2011-4354
CVE	CVE-2011-4576
CVE	CVE-2011-4577
CVE	CVE-2011-4619
CVE	CVE-2012-0027
CVE	CVE-2012-0050
XREF	USN:1357-1
XREF	IAVA:2011-A-0122
XREF	IAVA:2012-A-0009

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libssl0.9.8_0.9.8k-7ubuntu8.6
    Fixed package     : libssl0.9.8_0.9.8k-7ubuntu8.8

  - Installed package : openssl_0.9.8k-7ubuntu8.6
    Fixed package     : openssl_0.9.8k-7ubuntu8.8
```

57888 (1) - USN-1358-1 : php5 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that PHP computed hash values for form parameters without restricting the ability to trigger hash collisions predictably. This could allow a remote attacker to cause a denial of service by sending many crafted parameters. (CVE-2011-4885)
ATTENTION: this update changes previous PHP behavior by limiting the number of external input variables to 1000. This may be increased by adding a 'max_input_vars' directive to the php.ini configuration file. See http://www.php.net/manual/en/info.configuration.php#ini.max-input-var s for more information.
Stefan Esser discovered that the fix to address the predictable hash collision issue, CVE-2011-4885, did not properly handle the situation where the limit was reached. This could allow a remote attacker to cause a denial of service or execute arbitrary code via a request containing a large number of variables. (CVE-2012-0830)
It was discovered that PHP did not always check the return value of the zend_strndup function. This could allow a remote attacker to cause a denial of service. (CVE-2011-4153)
It was discovered that PHP did not properly enforce libxslt security settings. This could allow a remote attacker to create arbitrary files via a crafted XSLT stylesheet that uses the libxslt output extension. (CVE-2012-0057)
It was discovered that PHP did not properly enforce that PDORow objects could not be serialized and not be saved in a session. A remote attacker could use this to cause a denial of service via an application crash. (CVE-2012-0788)
It was discovered that PHP allowed the magic_quotes_gpc setting to be disabled remotely. This could allow a remote attacker to bypass restrictions that could prevent an SQL injection. (CVE-2012-0831)
USN 1126-1 addressed an issue where the /etc/cron.d/php5 cron job for PHP allowed local users to delete arbitrary files via a symlink attack on a directory under /var/lib/php5/. Emese Revfy discovered that the fix had not been applied to PHP for Ubuntu 10.04 LTS. This update corrects the issue. We apologize for the error.
(CVE-2011-0441)

See Also

http://www.ubuntu.com/usn/usn-1358-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2011-0441
CVE	CVE-2011-4153
CVE	CVE-2011-4885
CVE	CVE-2012-0057
CVE	CVE-2012-0788
CVE	CVE-2012-0830
CVE	CVE-2012-0831
XREF	USN:1358-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libapache2-mod-php5_5.3.2-1ubuntu4.9
    Fixed package     : libapache2-mod-php5_5.3.2-1ubuntu4.13

  - Installed package : php5_5.3.2-1ubuntu4.9
    Fixed package     : php5_5.3.2-1ubuntu4.13
```

```
- Installed package : php5-cli_5.3.2-1ubuntu4.9
  Fixed package     : php5-cli_5.3.2-1ubuntu4.13

- Installed package : php5-common_5.3.2-1ubuntu4.9
  Fixed package     : php5-common_5.3.2-1ubuntu4.13
```

57932 (1) - USN-1358-2 : php5 regression

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN 1358-1 fixed multiple vulnerabilities in PHP. The fix for CVE-2012-0831 introduced a regression where the state of the magic_quotes_gpc setting was not correctly reflected when calling the ini_get() function.
We apologize for the inconvenience.
Original advisory details:
It was discovered that PHP computed hash values for form parameters without restricting the ability to trigger hash collisions predictably. This could allow a remote attacker to cause a denial of service by sending many crafted parameters. (CVE-2011-4885) ATTENTION: this update changes previous PHP behavior by limiting the number of external input variables to 1000. This may be increased by adding a 'max_input_vars' directive to the php.ini configuration file. See http://www.php.net/manual/en/info.configuration.php#ini.max-input-var s for more information. Stefan Esser discovered that the fix to address the predictable hash collision issue, CVE-2011-4885, did not properly handle the situation where the limit was reached. This could allow a remote attacker to cause a denial of service or execute arbitrary code via a request containing a large number of variables. (CVE-2012-0830) It was discovered that PHP did not always check the return value of the zend_strndup function. This could allow a remote attacker to cause a denial of service. (CVE-2011-4153) It was discovered that PHP did not properly enforce libxslt security settings. This could allow a remote attacker to create arbitrary files via a crafted XSLT stylesheet that uses the libxslt output extension. (CVE-2012-0057) It was discovered that PHP did not properly enforce that PDORow objects could not be serialized and not be saved in a session. A remote attacker could use this to cause a denial of service via an application crash. (CVE-2012-0788) It was discovered that PHP allowed the magic_quotes_gpc setting to be disabled remotely. This could allow a remote attacker to bypass restrictions that could prevent an SQL injection. (CVE-2012-0831) USN 1126-1 addressed an issue where the /etc/cron.d/php5 cron job for PHP allowed local users to delete arbitrary files via a symlink attack on a directory under /var/lib/php5/. Emese Revfy discovered that the fix had not been applied to PHP for Ubuntu 10.04 LTS. This update corrects the issue. We apologize for the error. (CVE-2011-0441)

See Also

http://www.ubuntu.com/usn/usn-1358-2/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2011-0441
CVE	CVE-2011-4153
CVE	CVE-2011-4885
CVE	CVE-2012-0057
CVE	CVE-2012-0788
CVE	CVE-2012-0830
CVE	CVE-2012-0831
XREF	USN:1358-2

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libapache2-mod-php5_5.3.2-1ubuntu4.9
    Fixed package     : libapache2-mod-php5_5.3.2-1ubuntu4.14
```

```
- Installed package : php5_5.3.2-1ubuntu4.9
  Fixed package     : php5_5.3.2-1ubuntu4.14

- Installed package : php5-cli_5.3.2-1ubuntu4.9
  Fixed package     : php5-cli_5.3.2-1ubuntu4.14
```

57934 (1) - USN-1360-1 : firefox vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Andrew McCreight and Olli Pettay discovered a use-after-free vulnerability in the XBL bindings. An attacker could exploit this to cause a denial of service via application crash, or potentially execute code with the privileges of the user invoking Firefox.
(CVE-2012-0452)

See Also

http://www.ubuntu.com/usn/usn-1360-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2012-0452
XREF	USN:1360-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : firefox_9.0.1-bt0
    Fixed package     : firefox_10.0.1+build1-0ubuntu0.10.04.1
```

57997 (1) - USN-1284-2 : update-manager regression

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-1284-1 fixed vulnerabilities in Update Manager. One of the fixes introduced a regression for Kubuntu users attempting to upgrade to a newer Ubuntu release. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
David Black discovered that Update Manager incorrectly extracted the downloaded upgrade tarball before verifying its GPG signature. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could potentially be used to replace arbitrary files.
(CVE-2011-3152) David Black discovered that Update Manager created a temporary directory in an insecure fashion. A local attacker could possibly use this flaw to read the XAUTHORITY file of the user performing the upgrade.
(CVE-2011-3154) This update also adds a hotfix to Update Notifier to handle cases where the upgrade is being performed from CD media.

See Also

http://www.ubuntu.com/usn/usn-1284-2/

Solution

Update the affected package(s).

Risk Factor

High

References

CVE	CVE-2011-3152
CVE	CVE-2011-3154
XREF	USN:1284-2

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : update-manager-core_1:0.134.11
    Fixed package     : update-manager-core_1:0.134.11.2
```

57998 (1) - USN-1367-1 : libpng vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that libpng did not properly verify the embedded profile length of iCCP chunks. An attacker could exploit this to cause a denial of service via application crash. This issue only affected Ubuntu 8.04 LTS. (CVE-2009-5063)
Jueri Aedla discovered that libpng did not properly verify the size used when allocating memory during chunk decompression. If a user or automated system using libpng were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service or execute code with the privileges of the user invoking the program. (CVE-2011-3026)

See Also

http://www.ubuntu.com/usn/usn-1367-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2009-5063
CVE	CVE-2011-3026
XREF	USN:1367-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libpng12-0_1.2.42-1ubuntu2.1
    Fixed package     : libpng12-0_1.2.42-1ubuntu2.3
```

58034 (1) - USN-1367-2 : firefox vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-1367-1 fixed vulnerabilities in libpng. This provides the corresponding update for Firefox.
Original advisory details:
Jueri Aedla discovered that libpng did not properly verify the size used when allocating memory during chunk decompression. If a user or automated system using libpng were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service or execute code with the privileges of the user invoking the program. (CVE-2011-3026)

See Also

http://www.ubuntu.com/usn/usn-1367-2/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2011-3026
XREF	USN:1367-2

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : firefox_9.0.1-bt0
    Fixed package     : firefox_10.0.2+build1-0ubuntu0.10.04.1
```

58036 (1) - USN-1367-4 : xulrunner-1.9.2 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-1367-1 fixed vulnerabilities in libpng. This provides the corresponding update for Xulrunner.
Original advisory details:
Jueri Aedla discovered that libpng did not properly verify the size used when allocating memory during chunk decompression. If a user or automated system using libpng were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service or execute code with the privileges of the user invoking the program. (CVE-2011-3026)

See Also

http://www.ubuntu.com/usn/usn-1367-4/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2011-3026
XREF	USN:1367-4

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : xulrunner-1.9.2_1.9.2.17+build3+nobinonly-0ubuntu0.10.04.1
    Fixed package     : xulrunner-1.9.2_1.9.2.27+build1+nobinonly-0ubuntu0.10.04.1
```

58104 (1) - USN-1371-1 : cvs vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that cvs incorrectly handled certain responses from proxy servers. If a user were tricked into connecting to a malicious proxy server, a remote attacker could cause cvs to crash, or possibly execute arbitrary code.

See Also

http://www.ubuntu.com/usn/usn-1371-1/

Solution

Update the affected package(s).

Risk Factor

High

References

CVE	CVE-2012-0804
XREF	USN:1371-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : cvs_1:1.12.13-12ubuntu1
    Fixed package     : cvs_1:1.12.13-12ubuntu1.10.04.1
```

58144 (1) - USN-1375-1 : python-httplib2 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

The httplib2 Python library earlier than version 0.7.0 did not perform any server certificate validation when using HTTPS connections. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could be exploited to alter or compromise confidential information in applications that used the httplib2 library.

See Also

http://www.ubuntu.com/usn/usn-1375-1/

Solution

Update the affected package(s).

Risk Factor

High

References

XREF	USN:1375-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : python-httplib2_0.6.0-1
    Fixed package     : python-httplib2_0.7.2-1ubuntu2~0.10.04.1
```

58145 (1) - USN-1376-1 : libxml2 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Juraj Somorovsky discovered that libxml2 was vulnerable to hash table collisions. If a user or application linked against libxml2 were tricked into opening a specially crafted XML file, an attacker could cause a denial of service.

See Also

http://www.ubuntu.com/usn/usn-1376-1/

Solution

Update the affected package(s).

Risk Factor

High

References

CVE	CVE-2012-0841
XREF	USN:1376-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libxml2_2.7.6.dfsg-1ubuntu1.1
    Fixed package     : libxml2_2.7.6.dfsg-1ubuntu1.4
```

58146 (1) - USN-1377-1 : ruby1.8 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Drew Yao discovered that the WEBrick HTTP server was vulnerable to cross-site scripting attacks when displaying error pages. A remote attacker could use this flaw to run arbitrary web script.
(CVE-2010-0541)
Drew Yao discovered that Ruby's BigDecimal module did not properly allocate memory on 64-bit platforms. An attacker could use this flaw to cause a denial of service or possibly execute arbitrary code with user privileges.
(CVE-2011-0188)
Nicholas Jefferson discovered that the FileUtils.remove_entry_secure method in Ruby did not properly remove non-empty directories. An attacker could use this flaw to possibly delete arbitrary files.
(CVE-2011-1004)
It was discovered that Ruby incorrectly allowed untainted strings to be modified in protective safe levels. An attacker could use this flaw to bypass intended access restrictions. (CVE-2011-1005)
Eric Wong discovered that Ruby does not properly reseed its pseudorandom number generator when creating child processes. An attacker could use this flaw to gain knowledge of the random numbers used in other Ruby child processes. (CVE-2011-2686)
Eric Wong discovered that the SecureRandom module in Ruby did not properly seed its pseudorandom number generator. An attacker could use this flaw to gain knowledge of the random numbers used by another Ruby process with the same process ID number. (CVE-2011-2705)
Alexander Klink and Julian Wälde discovered that Ruby computed hash values without restricting the ability to trigger hash collisions predictably. A remote attacker could cause a denial of service by crafting values used in hash tables.
(CVE-2011-4815)

See Also

http://www.ubuntu.com/usn/usn-1377-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2010-0541
CVE	CVE-2011-0188
CVE	CVE-2011-1004
CVE	CVE-2011-1005
CVE	CVE-2011-2686
CVE	CVE-2011-2705
CVE	CVE-2011-4815
XREF	USN:1377-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libruby1.8_1.8.7.249-2
    Fixed package     : libruby1.8_1.8.7.249-2ubuntu0.1

  - Installed package : ruby1.8_1.8.7.249-2
    Fixed package     : ruby1.8_1.8.7.249-2ubuntu0.1
```

58168 (1) - USN-1378-1 : postgresql-8.3, postgresql-8.4, postgresql-9.1 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that PostgreSQL incorrectly checked permissions on functions called by a trigger. An attacker could attach a trigger to a table they owned and possibly escalate privileges. (CVE-2012-0866)
It was discovered that PostgreSQL incorrectly truncated SSL certificate name checks to 32 characters. If a host name was exactly 32 characters, this issue could be exploited by an attacker to spoof the SSL certificate. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, Ubuntu 11.04 and Ubuntu 11.10. (CVE-2012-0867)
It was discovered that the PostgreSQL pg_dump utility incorrectly filtered line breaks in object names. An attacker could create object names that execute arbitrary SQL commands when a dump script is reloaded. (CVE-2012-0868)

See Also

http://www.ubuntu.com/usn/usn-1378-1/

Solution

Update the affected package(s).

Risk Factor

High

References

CVE	CVE-2012-0866
CVE	CVE-2012-0867
CVE	CVE-2012-0868
XREF	USN:1378-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : postgresql-8.4_8.4.8-0ubuntu0.10.04
    Fixed package     : postgresql-8.4_8.4.11-0ubuntu0.10.04
```

58301 (1) - USN-1395-1 : python-pam vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Markus Vervier discovered that PyPAM incorrectly handled passwords containing NULL bytes. An attacker could exploit this to cause applications using PyPAM to crash, or possibly execute arbitrary code.

See Also

http://www.ubuntu.com/usn/usn-1395-1/

Solution

Update the affected package(s).

Risk Factor

High

References

CVE	CVE-2012-1502
XREF	USN:1395-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : python-pam_0.4.2-12.1ubuntu1
    Fixed package     : python-pam_0.4.2-12.1ubuntu1.10.04.1
```

58318 (1) - USN-1396-1 : eglibc, glibc vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that the GNU C Library did not properly handle integer overflows in the timezone handling code. An attacker could use this to possibly execute arbitrary code by convincing an application to load a maliciously constructed tzfile. (CVE-2009-5029)
It was discovered that the GNU C Library did not properly handle passwd.adjunct.byname map entries in the Network Information Service (NIS) code in the name service caching daemon (nscd). An attacker could use this to obtain the encrypted passwords of NIS accounts.
This issue only affected Ubuntu 8.04 LTS. (CVE-2010-0015)
Chris Evans reported that the GNU C Library did not properly calculate the amount of memory to allocate in the fnmatch() code. An attacker could use this to cause a denial of service or possibly execute arbitrary code via a maliciously crafted UTF-8 string. This issue only affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS and Ubuntu 10.10. (CVE-2011-1071)
Tomas Hoger reported that an additional integer overflow was possible in the GNU C Library fnmatch() code. An attacker could use this to cause a denial of service via a maliciously crafted UTF-8 string.
This issue only affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-1659)
Dan Rosenberg discovered that the addmntent() function in the GNU C Library did not report an error status for failed attempts to write to the /etc/mtab file. This could allow an attacker to corrupt /etc/mtab, possibly causing a denial of service or otherwise manipulate mount options. This issue only affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-1089)
Harald van Dijk discovered that the locale program included with the GNU C library did not properly quote its output. This could allow a local attacker to possibly execute arbitrary code using a crafted localization string that was evaluated in a shell script. This issue only affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS and Ubuntu 10.10. (CVE-2011-1095)
It was discovered that the GNU C library loader expanded the $ORIGIN dynamic string token when RPATH is composed entirely of this token.
This could allow an attacker to gain privilege via a setuid program that had this RPATH value. (CVE-2011-1658)
It was discovered that the GNU C library implementation of memcpy optimized for Supplemental Streaming SIMD Extensions 3 (SSSE3) contained a possible integer overflow. An attacker could use this to cause a denial of service or possibly execute arbitrary code. This issue only affected Ubuntu 10.04 LTS. (CVE-2011-2702)
John Zimmerman discovered that the Remote Procedure Call (RPC) implementation in the GNU C Library did not properly handle large numbers of connections. This could allow a remote attacker to cause a denial of service. (CVE-2011-4609)
It was discovered that the GNU C Library vfprintf() implementation contained a possible integer overflow in the format string protection code offered by FORTIFY_SOURCE. An attacker could use this flaw in conjunction with a format string vulnerability to bypass the format string protection and possibly execute arbitrary code. (CVE-2012-0864)

See Also

http://www.ubuntu.com/usn/usn-1396-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2009-5029
CVE	CVE-2010-0015
CVE	CVE-2011-1071
CVE	CVE-2011-1089
CVE	CVE-2011-1095

CVE	CVE-2011-1658
CVE	CVE-2011-1659
CVE	CVE-2011-2702
CVE	CVE-2011-4609
CVE	CVE-2012-0864
XREF	USN:1396-1
XREF	CWE:255

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libc-bin_2.11.1-0ubuntu7.8
    Fixed package     : libc-bin_2.11.1-0ubuntu7.10

  - Installed package : libc6_2.11.1-0ubuntu7.8
    Fixed package     : libc6_2.11.1-0ubuntu7.10
```

58325 (1) - USN-1397-1 : mysql-5.1, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.
MySQL has been updated to 5.1.61 in Ubuntu 10.04 LTS, Ubuntu 10.10, Ubuntu 11.04 and Ubuntu 11.10. Ubuntu 8.04 LTS has been updated to MySQL 5.0.95.
In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.
Please see the following for more information:
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-x.html http://dev.mysql.com/doc/refman/5.0/en/news-5-0-x.html
http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.h tml

See Also

http://www.ubuntu.com/usn/usn-1397-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2007-5925
CVE	CVE-2008-3963
CVE	CVE-2008-4098
CVE	CVE-2008-4456
CVE	CVE-2008-7247
CVE	CVE-2009-2446
CVE	CVE-2009-4019
CVE	CVE-2009-4030
CVE	CVE-2009-4484
CVE	CVE-2010-1621
CVE	CVE-2010-1626
CVE	CVE-2010-1848
CVE	CVE-2010-1849
CVE	CVE-2010-1850
CVE	CVE-2010-2008
CVE	CVE-2010-3677
CVE	CVE-2010-3678

CVE	CVE-2010-3679
CVE	CVE-2010-3680
CVE	CVE-2010-3681
CVE	CVE-2010-3682
CVE	CVE-2010-3683
CVE	CVE-2010-3833
CVE	CVE-2010-3834
CVE	CVE-2010-3835
CVE	CVE-2010-3836
CVE	CVE-2010-3837
CVE	CVE-2010-3838
CVE	CVE-2010-3839
CVE	CVE-2010-3840
CVE	CVE-2011-2262
CVE	CVE-2012-0075
CVE	CVE-2012-0087
CVE	CVE-2012-0101
CVE	CVE-2012-0102
CVE	CVE-2012-0112
CVE	CVE-2012-0113
CVE	CVE-2012-0114
CVE	CVE-2012-0115
CVE	CVE-2012-0116
XREF	USN:1397-1
XREF	CWE:119

Exploitable with

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

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : mysql-server-5.1_5.1.41-3ubuntu12.10
    Fixed package     : mysql-server-5.1_5.1.61-0ubuntu0.10.04.1
```

12218 (4) - mDNS Detection

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

Solution

Filter incoming traffic to UDP port 5353 if desired.

Risk Factor

Medium

CVSS Base Score

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

Hosts

192.168.1.13 (udp/5353)

```
Nessus was able to extract the following information :

  - mDNS hostname       : gogo.local.

  - Advertised services :
    o Service name      : gogo [00:a0:cc:3d:b3:ba]._workstation._tcp.local.
      Port number       : 9

  - CPU type            : I686
  - OS                  : LINUX
```

192.168.1.30 (udp/5353)

```
Nessus was able to extract the following information :

  - mDNS hostname       : NAS-BASEMENT.local.

  - Advertised services :
    o Service name      : NAS-BASEMENT [00:0d:a2:01:83:fb]._workstation._tcp.local.
      Port number       : 9
    o Service name      : ReadyNAS Discovery [NAS-BASEMENT]._readynas._tcp.local.
      Port number       : 9
    o Service name      : NAS-BASEMENT (CIFS)._smb._tcp.local.
      Port number       : 139
    o Service name      : NAS-BASEMENT (AFP)._afpovertcp._tcp.local.
      Port number       : 548

  - CPU type            : PADRE
  - OS                  : LINUX
```

192.168.1.81 (udp/5353)

```
Nessus was able to extract the following information :

  - mDNS hostname       : DVR-E613.local.

  - Advertised services :
    o Service name      : DVR-E613._tivo-device._tcp.local.
      Port number       : 80
    o Service name      : DVR-E613._tivo-videos._tcp.local.
      Port number       : 443
    o Service name      : DVR-E613._tivo-videostream._tcp.local.
      Port number       : 443
    o Service name      : DVR-E613._http._tcp.local.
      Port number       : 80
```

192.168.1.211 (udp/5353)

```
Nessus was able to extract the following information :

  - mDNS hostname       : AppleTV.local.
  - Advertised services :
    o Service name      : 70-35-10-73 AppleTV._sleep-proxy._udp.local.
      Port number       : 57768
    o Service name      : 76A17F1F1E099ACB._appletv._tcp.local.
      Port number       : 3689
    o Service name      : 76A17F1F1E099ACB._touch-able._tcp.local.
      Port number       : 3689
    o Service name      : iTunes_Ctrl_8EFC296D77A471B5._dacp._tcp.local.
      Port number       : 3689
```

12217 (3) - DNS Server Cache Snooping Remote Information Disclosure

Synopsis

The remote DNS server is vulnerable to cache snooping attacks.

Description

The remote DNS server responds to queries for third-party domains that do not have the recursion bit set.
This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.
For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.
Note: If this is an internal DNS server not accessable to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.

See Also

http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf

Solution

Contact the vendor of the DNS software for a fix.

Risk Factor

Medium

CVSS Base Score

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

Hosts

192.168.1.10 (udp/53)

```
Nessus sent a non-recursive query for example.com
and received 1 answer :

192.0.43.10
```

192.168.1.78 (udp/53)

```
Nessus sent a non-recursive query for example.com
and received 1 answer :

192.0.43.10
```

192.168.1.79 (udp/53)

```
Nessus sent a non-recursive query for example.com
and received 1 answer :

192.0.43.10
```

57792 (3) - Apache HTTP Server httpOnly Cookie Information Disclosure

Synopsis

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

Description

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

See Also

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

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

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

Solution

Upgrade to Apache version 2.2.22 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

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

Hosts

192.168.1.30 (tcp/80)
192.168.1.30 (tcp/443)
192.168.1.248 (tcp/80)

10595 (2) - DNS Server Zone Transfer Information Disclosure (AXFR)

Synopsis

The remote name server allows zone transfers

Description

The remote name server allows DNS zone transfers to be performed.
A zone transfer lets a remote attacker instantly populate a list of potential targets. In addition, companies often use a naming convention that can give hints as to a servers primary application (for instance, proxy.example.com, payroll.example.com, b2b.example.com, etc.).
As such, this information is of great use to an attacker, who may use it to gain information about the topology of the network and spot new targets.

See Also

http://en.wikipedia.org/wiki/AXFR

Solution

Limit DNS zone transfers to only the servers that need the information.

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-1999-0532
XREF	OSVDB:492

Hosts

192.168.1.10 (tcp/53)
192.168.1.79 (tcp/53)

42873 (2) - SSL Medium Strength Cipher Suites Supported

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, which we currently regard as those with key lengths at least 56 bits and less than 112 bits.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS Base Score

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

Hosts

192.168.1.13 (tcp/1243)

```
Here is the list of medium strength SSL ciphers supported by the remote server :

  Medium Strength Ciphers (>= 56-bit and < 112-bit key)
    TLSv1
      DES-CBC-SHA                Kx=RSA         Au=RSA      Enc=DES(56)         Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

192.168.1.81 (tcp/443)

```
Here is the list of medium strength SSL ciphers supported by the remote server :

  Medium Strength Ciphers (>= 56-bit and < 112-bit key)
    SSLv3
      DES-CBC-SHA                Kx=RSA         Au=RSA      Enc=DES(56)         Mac=SHA1
    TLSv1
      DES-CBC-SHA                Kx=RSA         Au=RSA      Enc=DES(56)         Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

51192 (2) - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.
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 was not possible to verify. 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 nullifies the use of SSL as anyone could establish a man in the middle attack against the remote host.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Hosts

192.168.1.81 (tcp/443)

```

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : CN=746-0001-9022-E613/O=TiVo Inc./OU=IT/L=Alviso/ST=California/C=US
|-Issuer  : CN=746-0001-9022-E613/O=TiVo Inc./OU=IT/L=Alviso/ST=California/C=US
```

192.168.1.231 (tcp/1241)

```

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/
CN=Nessus Certification Authority
|-Issuer  : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/
CN=Nessus Certification Authority
```

57582 (2) - 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 certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Hosts

192.168.1.81 (tcp/443)

```
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 : CN=746-0001-9022-E613/O=TiVo Inc./OU=IT/L=Alviso/ST=California/C=US
```

192.168.1.231 (tcp/1241)

```
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 : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/
CN=Nessus Certification Authority
```

57608 (2) - SMB Signing Disabled

Synopsis

Signing is disabled on the remote SMB server.

Description

Signing is disabled on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.

See Also

http://support.microsoft.com/kb/887429

http://www.nessus.org/u?74b80723

http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS Base Score

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

Hosts

192.168.1.16 (tcp/445)

192.168.1.30 (tcp/445)

18262 (1) - TFTP Traversal Arbitrary File Access

Synopsis

The remote TFTP server can be used to read arbitrary files on the remote host.

Description

The TFTP (Trivial File Transfer Protocol) server running on the remote host is vulnerable to a directory traversal attack that allows an attacker to read arbitrary files on the remote host by prepending their names with directory traversal sequences.

Solution

Disable the remote TFTP daemon, run it in a chrooted environment, or filter incoming traffic to this port.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	6198
BID	11582
BID	11584
BID	33287
BID	33344
BID	42907
BID	48272
BID	50441
CVE	CVE-1999-0183
CVE	CVE-1999-0498
CVE	CVE-2002-2353
CVE	CVE-2009-0271
CVE	CVE-2009-0288
CVE	CVE-2009-1161
XREF	OSVDB:8069
XREF	OSVDB:11221
XREF	OSVDB:11297
XREF	OSVDB:11349
XREF	OSVDB:51404
XREF	OSVDB:51487

XREF	OSVDB:57701
XREF	OSVDB:76743
XREF	EDB-ID:14857
XREF	EDB-ID:17507
XREF	CWE:22

Exploitable with

CANVAS (true)

Hosts

192.168.1.80 (udp/69)

```
It was possible to retrieve the contents of the file
/etc/passwd from the remote host :

root:x:0:0:root:/root:/bin/sh
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:100:sync:/bin:/bin/sync
mail:x:8:8:mail:/var/spool/mail:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
operator:x:37:37:Operator:/var:/bin/sh
sshd:x:103:99:Operator:/var:/bin/sh
nobody:x:99:99:nobody:/home:/bin/sh
default:x:1000:1000:Default non-root user:/home/default:/bin/sh
```

18405 (1) - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

Synopsis

It may be possible to get access to the remote host.

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.
This flaw exists because the RDP server stores a hardcoded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

See Also

http://www.oxid.it/downloads/rdp-gbu.pdf

http://technet.microsoft.com/en-us/library/cc782610.aspx

Solution

- Force the use of SSL as a transport layer for this service if supported, or/and
- Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	13818
CVE	CVE-2005-1794
XREF	OSVDB:17131

Hosts

192.168.1.16 (tcp/3389)

26919 (1) - Microsoft Windows SMB Guest Account Local User Access

Synopsis

It is possible to log into the remote host.

Description

The remote host is running one of the Microsoft Windows operating systems. It was possible to log into it as a guest user using a random account.

Solution

In the group policy change the setting for 'Network access: Sharing and security model for local accounts' from 'Guest only - local users authenticate as Guest' to 'Classic - local users authenticate as themselves'.

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-1999-0505

Hosts

192.168.1.30 (tcp/445)

42256 (1) - NFS Shares World Readable

Synopsis

The remote NFS server exports world readable shares.

Description

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

See Also

http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

Solution

Place the appropriate restrictions on all NFS shares.

Risk Factor

Medium

CVSS Base Score

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

References

XREF	OSVDB:339

Hosts

192.168.1.30 (tcp/2049)

```

The following shares have no access restrictions :

  /c/backup *
  /c/media *
```

43156 (1) - NTP ntpd Mode 7 Error Response Packet Loop Remote DoS

Synopsis

The remote network time service has a denial of service vulnerability.

Description

The version of ntpd running on the remote host has a denial of service vulnerability. It responds to mode 7 error packets with its own mode 7 error packets. A remote attacker could exploit this by sending a mode 7 error response with a spoofed IP header, setting the source and destination IP addresses to the IP address of the target. This would cause ntpd to respond to itself endlessly, consuming excessive amounts of CPU, resulting in a denial of service.

See Also

https://support.ntp.org/bugs/show_bug.cgi?id=1331

http://www.nessus.org/u?3a07ed05

Solution

Upgrade to NTP 4.2.4p8 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	37255
CVE	CVE-2009-3563
XREF	OSVDB:60847
XREF	CERT:568372
XREF	Secunia:37629

Hosts

192.168.1.211 (udp/123)

45374 (1) - AFP Server Directory Traversal

Synopsis

The remote service is vulnerable to an information disclosure attack.

Description

The remote AFP server allows guest users to read files located outside public shares by sending requests to the '..' directory.
An attacker could use this flaw to read every file on this host.

See Also

http://support.apple.com/kb/HT4077

http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html

http://www.securityfocus.com/advisories/19364

Solution

Upgrade to Mac OS X 10.6.3 or apply Security Update 2010-002.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	39020
CVE	CVE-2010-0533
XREF	OSVDB:63366

Hosts

192.168.1.30 (tcp/548)

```
It was possible to obtain a listing of '..' for the share 'media' :
 - lost+found
 - backup
 - home
 - .timemachine
 - .vault
 - media
 - aquota.group
 - aquota.user
```

52740 (1) - USN-1090-1 : linux vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Dan Rosenberg discovered that multiple terminal ioctls did not correctly initialize structure memory. A local attacker could exploit this to read portions of kernel stack memory, leading to a loss of privacy. (CVE-2010-4076, CVE-2010-4077)
Dan Rosenberg discovered that the socket filters did not correctly initialize structure memory. A local attacker could create malicious filters to read portions of kernel stack memory, leading to a loss of privacy. (Ubuntu 10.10 was already fixed in a prior update.) (CVE-2010-4158)
Dan Rosenberg discovered that the SCSI subsystem did not correctly validate iov segments. A local attacker with access to a SCSI device could send specially crafted requests to crash the system, leading to a denial of service. (CVE-2010-4163)
Dan Rosenberg discovered that the RDS protocol did not correctly check ioctl arguments. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-4175)

See Also

http://www.ubuntu.com/usn/usn-1090-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2010-4076
CVE	CVE-2010-4077
CVE	CVE-2010-4158
CVE	CVE-2010-4163
CVE	CVE-2010-4175
XREF	USN:1090-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : linux-libc-dev_2.6.32-29.58
    Fixed package     : linux-libc-dev_2.6.32-30.59
```

55095 (1) - USN-1134-1 : apache2, apr vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Maksymilian Arciemowicz reported that a flaw in the fnmatch() implementation in the Apache Portable Runtime (APR) library could allow an attacker to cause a denial of service. This can be demonstrated in a remote denial of service attack against mod_autoindex in the Apache web server. (CVE-2011-0419)
Is was discovered that the fix for CVE-2011-0419 introduced a different flaw in the fnmatch() implementation that could also result in a denial of service. (CVE-2011-1928)

See Also

http://www.ubuntu.com/usn/usn-1134-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-0419
CVE	CVE-2011-1928
XREF	USN:1134-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libapr1_1.3.8-1build1
    Fixed package     : libapr1_1.3.8-1ubuntu0.3
```

55097 (1) - USN-1136-1 : rdesktop vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that rdesktop incorrectly handled specially crafted paths when using disk redirection. If a user were tricked into connecting to a malicious server, an attacker could access arbitrary files on the user's filesystem.

See Also

http://www.ubuntu.com/usn/usn-1136-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-1595
XREF	USN:1136-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : rdesktop_1.6.0-2ubuntu3
    Fixed package     : rdesktop_1.6.0-2ubuntu3.1
```

55101 (1) - USN-1139-1 : bind9 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that Bind incorrectly handled certain bad signatures if multiple trust anchors existed for a single zone. A remote attacker could use this flaw to cause Bind to stop responding, resulting in a denial of service. This issue only affected Ubuntu 8.04 LTS and 10.04 LTS. (CVE-2010-3762)
Frank Kloeker and Michael Sinatra discovered that Bind incorrectly handled certain very large RRSIG RRsets included in negative responses. A remote attacker could use this flaw to cause Bind to stop responding, resulting in a denial of service. (CVE-2011-1910)

See Also

http://www.ubuntu.com/usn/usn-1139-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2010-3762
CVE	CVE-2011-1910
XREF	USN:1139-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libdns64_1:9.7.0.dfsg.P1-1ubuntu0.1
    Fixed package     : libdns64_1:9.7.0.dfsg.P1-1ubuntu0.2
```

55102 (1) - USN-1140-1 : pam vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Marcus Granado discovered that PAM incorrectly handled configuration files with non-ASCII usernames. A remote attacker could use this flaw to cause a denial of service, or possibly obtain login access with a different users username. This issue only affected Ubuntu 8.04 LTS.
(CVE-2009-0887)
It was discovered that the PAM pam_xauth, pam_env and pam_mail modules incorrectly handled dropping privileges when performing operations. A local attacker could use this flaw to read certain arbitrary files, and access other sensitive information.
(CVE-2010-3316, CVE-2010-3430, CVE-2010-3431, CVE-2010-3435)
It was discovered that the PAM pam_namespace module incorrectly cleaned the environment during execution of the namespace.init script. A local attacker could use this flaw to possibly gain privileges. (CVE-2010-3853)
It was discovered that the PAM pam_xauth module incorrectly handled certain failures. A local attacker could use this flaw to delete certain unintended files. (CVE-2010-4706)
It was discovered that the PAM pam_xauth module incorrectly verified certain file properties. A local attacker could use this flaw to cause a denial of service. (CVE-2010-4707)

See Also

http://www.ubuntu.com/usn/usn-1140-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2009-0887
CVE	CVE-2010-3316
CVE	CVE-2010-3430
CVE	CVE-2010-3431
CVE	CVE-2010-3435
CVE	CVE-2010-3853
CVE	CVE-2010-4706
CVE	CVE-2010-4707
XREF	USN:1140-1
XREF	CWE:189

Hosts

192.168.1.248 (tcp/0)

```
- Installed package : libpam-modules_1.1.1-2ubuntu5.1
  Fixed package     : libpam-modules_1.1.1-2ubuntu5.2
```

55103 (1) - USN-1140-2 : pam regression

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-1140-1 fixed vulnerabilities in PAM. A regression was found that caused cron to stop working with a 'Module is unknown' error. As a result, systems configured with automatic updates will not receive updates until cron is restarted, these updates are installed or the system is rebooted. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Marcus Granado discovered that PAM incorrectly handled configuration files with non-ASCII usernames. A remote attacker could use this flaw to cause a denial of service, or possibly obtain login access with a different users username. This issue only affected Ubuntu 8.04 LTS.
(CVE-2009-0887) It was discovered that the PAM pam_xauth, pam_env and pam_mail modules incorrectly handled dropping privileges when performing operations. A local attacker could use this flaw to read certain arbitrary files, and access other sensitive information.
(CVE-2010-3316, CVE-2010-3430, CVE-2010-3431, CVE-2010-3435) It was discovered that the PAM pam_namespace module incorrectly cleaned the environment during execution of the namespace.init script. A local attacker could use this flaw to possibly gain privileges. (CVE-2010-3853) It was discovered that the PAM pam_xauth module incorrectly handled certain failures. A local attacker could use this flaw to delete certain unintended files.
(CVE-2010-4706) It was discovered that the PAM pam_xauth module incorrectly verified certain file properties. A local attacker could use this flaw to cause a denial of service. (CVE-2010-4707)

See Also

http://www.ubuntu.com/usn/usn-1140-2/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2009-0887
CVE	CVE-2010-3316
CVE	CVE-2010-3430
CVE	CVE-2010-3431
CVE	CVE-2010-3435
CVE	CVE-2010-3853
CVE	CVE-2010-4706
CVE	CVE-2010-4707
XREF	USN:1140-2
XREF	CWE:189

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libpam-modules_1.1.1-2ubuntu5.1
    Fixed package     : libpam-modules_1.1.1-2ubuntu5.3

  - Installed package : libpam0g_1.1.1-2ubuntu5.1
    Fixed package     : libpam0g_1.1.1-2ubuntu5.3
```

55114 (1) - USN-1148-1 : libmodplug vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that libmodplug did not correctly handle certain malformed S3M media files. If a user or automated system were tricked into opening a crafted S3M file, an attacker could cause a denial of service or possibly execute arbitrary code with privileges of the user invoking the program. (CVE-2011-1574)
It was discovered that libmodplug did not correctly handle certain malformed ABC media files. If a user or automated system were tricked into opening a crafted ABC file, an attacker could cause a denial of service or possibly execute arbitrary code with privileges of the user invoking the program. (CVE-2011-1761)
The default compiler options for affected releases should reduce the vulnerability to a denial of service.

See Also

http://www.ubuntu.com/usn/usn-1148-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-1574
CVE	CVE-2011-1761
XREF	USN:1148-1

Exploitable with

CANVAS (true)Metasploit (true)

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libmodplug0c2_1:0.8.7-1build1
    Fixed package     : libmodplug0c2_1:0.8.7-1ubuntu0.2
```

55522 (1) - USN-1163-1 : bind9 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that Bind incorrectly handled certain specially crafted packets. A remote attacker could use this flaw to cause Bind to stop responding, resulting in a denial of service.

See Also

http://www.ubuntu.com/usn/usn-1163-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-2464
XREF	USN:1163-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libdns64_1:9.7.0.dfsg.P1-1ubuntu0.1
    Fixed package     : libdns64_1:9.7.0.dfsg.P1-1ubuntu0.3
```

55648 (1) - USN-1172-1 : logrotate vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that logrotate incorrectly handled the creation of new log files. Local users could possibly
read log files if they were opened before permissions were in place. This issue only affected Ubuntu 8.04 LTS.
(CVE-2011-1098)
It was discovered that logrotate incorrectly handled certain log file names when used with the shred option. Local attackers able to create log files with specially crafted filenames could use this issue to execute arbitrary code. This issue only affected Ubuntu 10.04 LTS, 10.10, and 11.04. (CVE-2011-1154)
It was discovered that logrotate incorrectly handled certain malformed log filenames. Local attackers able to create log files with specially crafted filenames could use this issue to cause logrotate to stop processing log files, resulting in a denial of service. (CVE-2011-1155)
It was discovered that logrotate incorrectly handled symlinks and hard links when processing log files. A local attacker having write access to a log file directory could use this issue to overwrite or read arbitrary files. This issue only affected Ubuntu 8.04 LTS.
(CVE-2011-1548)

See Also

http://www.ubuntu.com/usn/usn-1172-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-1098
CVE	CVE-2011-1154
CVE	CVE-2011-1155
CVE	CVE-2011-1548
XREF	USN:1172-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : logrotate_3.7.8-4ubuntu2.1
    Fixed package     : logrotate_3.7.8-4ubuntu2.2
```

55689 (1) - USN-1174-1 : libsndfile vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Hossein Lotfi discovered that libsndfile did not properly verify the header length and number of channels for PARIS Audio Format (PAF) audio files. An attacker could exploit this to cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program.

See Also

http://www.ubuntu.com/usn/usn-1174-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-2696
XREF	USN:1174-1

Hosts

192.168.1.248 (tcp/0)

```
- Installed package : libsndfile1_1.0.21-2
  Fixed package     : libsndfile1_1.0.21-2ubuntu0.10.04.1
```

55699 (1) - USN-1175-1 : libpng vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Frank Busse discovered that libpng did not properly handle certain malformed PNG images. If a user or automated system were tricked into opening a crafted PNG file, an attacker could cause libpng to crash, resulting in a denial of service. This issue only affected Ubuntu 10.04 LTS, 10.10, and 11.04. (CVE-2011-2501)
It was discovered that libpng did not properly handle certain malformed PNG images. If a user or automated system were tricked into opening a crafted PNG file, an attacker could cause a denial of service or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-2690)
Frank Busse discovered that libpng did not properly handle certain PNG images with invalid sCAL chunks. If a user or automated system were tricked into opening a crafted PNG file, an attacker could cause a denial of service or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-2692)

See Also

http://www.ubuntu.com/usn/usn-1175-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-2501
CVE	CVE-2011-2690
CVE	CVE-2011-2692
XREF	USN:1175-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libpng12-0_1.2.42-1ubuntu2.1
    Fixed package     : libpng12-0_1.2.42-1ubuntu2.2
```

55700 (1) - USN-1176-1 : dbus vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that DBus did not properly validate the byte order of messages under certain circumstances. An attacker could exploit this to cause a denial of service via application crash or potentially obtain access to sensitive information.

See Also

http://www.ubuntu.com/usn/usn-1176-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-2200
XREF	USN:1176-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : dbus_1.2.16-2ubuntu4.2
    Fixed package     : dbus_1.2.16-2ubuntu4.3
```

55731 (1) - USN-1181-1 : libsoup2.4 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that libsoup did not properly validate its input when processing SoupServer requests. A remote attacker could exploit this to access files via directory traversal.

See Also

http://www.ubuntu.com/usn/usn-1181-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-2524
XREF	USN:1181-1

Hosts

192.168.1.248 (tcp/0)

```
- Installed package : libsoup2.4-1_2.30.2-0ubuntu0.1
  Fixed package     : libsoup2.4-1_2.30.2-0ubuntu0.2
```

55957 (1) - USN-1194-1 : foomatic-filters vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that the foomatic-rip Foomatic filter incorrectly handled command-line options. An attacker could use this flaw to cause Foomatic to execute arbitrary code as the 'lp' user.

In the default installation, attackers would be isolated by the CUPS AppArmor profile.

See Also

http://www.ubuntu.com/usn/usn-1194-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-2697
CVE	CVE-2011-2964
XREF	USN:1194-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : foomatic-filters_4.0.4-0ubuntu1
    Fixed package     : foomatic-filters_4.0.4-0ubuntu1.1
```

56048 (1) - USN-1199-1 : apache2 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

A flaw was discovered in the byterange filter in Apache. A remote attacker could exploit this to cause a denial of service via resource exhaustion.

See Also

http://www.ubuntu.com/usn/usn-1199-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-3192
XREF	IAVA:2011-A-0120
XREF	USN:1199-1

Hosts

192.168.1.248 (tcp/0)

```
    - Installed package : apache2.2-bin_2.2.14-5ubuntu8.4
      Fixed package     : apache2.2-bin_2.2.14-5ubuntu8.6
```

56206 (1) - USN-1207-1 : cups, cupsys vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Tomas Hoger discovered that the CUPS image library incorrectly handled LZW streams. A remote attacker could use this flaw to cause a denial of service or possibly execute arbitrary code.

See Also

http://www.ubuntu.com/usn/usn-1207-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-2896
CVE	CVE-2011-3170
XREF	USN:1207-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libcupsimage2_1.4.3-1ubuntu1.4
    Fixed package     : libcupsimage2_1.4.3-1ubuntu1.5
```

56506 (1) - USN-1229-1 : postgresql-8.3, postgresql-8.4 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that the blowfish algorithm in the pgcrypto module incorrectly handled certain 8-bit characters, resulting in the password hashes being easier to crack than expected. An attacker who could obtain the password hashes would be able to recover the plaintext with less effort.

See Also

http://www.ubuntu.com/usn/usn-1229-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-2483
XREF	USN:1229-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : postgresql-8.4_8.4.8-0ubuntu0.10.04
    Fixed package     : postgresql-8.4_8.4.9-0ubuntu0.10.04
```

56778 (1) - USN-1259-1 : apache2, apache2-mpm-itk vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that the mod_proxy module in Apache did not properly interact with the RewriteRule and ProxyPassMatch pattern matches in the configuration of a reverse proxy. This could allow remote attackers to contact internal webservers behind the proxy that were not intended for external exposure. (CVE-2011-3368)
Stefano Nichele discovered that the mod_proxy_ajp module in Apache when used with mod_proxy_balancer in certain configurations could allow remote attackers to cause a denial of service via a malformed HTTP request. (CVE-2011-3348)
Samuel Montosa discovered that the ITK Multi-Processing Module for Apache did not properly handle certain configuration sections that specify NiceValue but not AssignUserID, preventing Apache from dropping privileges correctly. This issue only affected Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-1176)
USN 1199-1 fixed a vulnerability in the byterange filter of Apache.
The upstream patch introduced a regression in Apache when handling specific byte range requests. This update fixes the issue.
Original advisory details:
A flaw was discovered in the byterange filter in Apache. A remote attacker could exploit this to cause a denial of service via resource exhaustion.

See Also

http://www.ubuntu.com/usn/usn-1259-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-1176
CVE	CVE-2011-3348
CVE	CVE-2011-3368
XREF	USN:1259-1
XREF	IAVA:2012-A-0017

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : apache2.2-bin_2.2.14-5ubuntu8.4
    Fixed package     : apache2.2-bin_2.2.14-5ubuntu8.7
```

56861 (1) - USN-1264-1 : bind9 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that Bind incorrectly handled certain specially crafted packets. A remote attacker could use this flaw to cause Bind to crash, resulting in a denial of service.

See Also

http://www.ubuntu.com/usn/usn-1264-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-4313
XREF	IAVA:2011-A-0158
XREF	USN:1264-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libdns64_1:9.7.0.dfsg.P1-1ubuntu0.1
    Fixed package     : libdns64_1:9.7.0.dfsg.P1-1ubuntu0.4
```

57314 (1) - USN-1307-1 : php5 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Florent Hochwelker discovered that PHP incorrectly handled certain EXIF headers in JPEG files. A remote attacker could exploit this issue to view sensitive information or cause the PHP server to crash.

See Also

http://www.ubuntu.com/usn/usn-1307-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-4566
XREF	USN:1307-1

Hosts

192.168.1.248 (tcp/0)

```
- Installed package : php5-cli_5.3.2-1ubuntu4.9
  Fixed package     : php5-cli_5.3.2-1ubuntu4.11
```

57345 (1) - USN-1314-1 : python3.1, python3.2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Giampaolo Rodola discovered that the smtpd module in Python 3 did not properly handle certain error conditions. A remote attacker could exploit this to cause a denial of service via daemon outage. This issue only affected Ubuntu 10.04 LTS. (CVE-2010-3493)
Niels Heinen discovered that the urllib module in Python 3 would process Location headers that specify a file:// URL. A remote attacker could use this to obtain sensitive information or cause a denial of service via resource consumption. (CVE-2011-1521)

See Also

http://www.ubuntu.com/usn/usn-1314-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2010-3493
CVE	CVE-2011-1521
XREF	USN:1314-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : python3.1-minimal_3.1.2-0ubuntu3
    Fixed package     : python3.1-minimal_3.1.2-0ubuntu3.1
```

57357 (1) - USN-1315-1 : jasper vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Jonathan Foote discovered that JasPer incorrectly handled certain malformed JPEG-2000 image files. If a user were tricked into opening a specially crafted JPEG-2000 image file, a remote attacker could cause JasPer to crash or possibly execute arbitrary code with user privileges.

See Also

http://www.ubuntu.com/usn/usn-1315-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-4516
CVE	CVE-2011-4517
XREF	USN:1315-1

Hosts

192.168.1.248 (tcp/0)

```
- Installed package : libjasper1_1.900.1-7
  Fixed package     : libjasper1_1.900.1-7ubuntu0.10.04.1
```

57370 (1) - USN-1316-1 : t1lib vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Jonathan Brossard discovered that t1lib did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause t1lib to crash or possibly execute arbitrary code with user privileges.

See Also

http://www.ubuntu.com/usn/usn-1316-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-0764
XREF	USN:1316-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libt1-5_5.1.2-3build1
    Fixed package     : libt1-5_5.1.2-3ubuntu0.10.04.1
```

57690 (1) - Terminal Services Encryption Level is Medium or Low

Synopsis

The remote host is using weak cryptography.

Description

The remote Terminal Services service is not configured to use strong cryptography.
Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.

Solution

Change RDP encryption level to one of :
3. High
4. FIPS Compliant

Risk Factor

Medium

CVSS Base Score

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

Hosts

192.168.1.16 (tcp/3389)

```
The terminal services encryption level is set to :

2. Medium
```

57999 (1) - USN-1368-1 : apache2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that the Apache HTTP Server incorrectly handled the SetEnvIf .htaccess file directive. An attacker having write access to a .htaccess file may exploit this to possibly execute arbitrary code.
(CVE-2011-3607)
Prutha Parikh discovered that the mod_proxy module did not properly interact with the RewriteRule and ProxyPassMatch pattern matches in the configuration of a reverse proxy. This could allow remote attackers to contact internal webservers behind the proxy that were not intended for external exposure. (CVE-2011-4317)
Rainer Canavan discovered that the mod_log_config module incorrectly handled a certain format string when used with a threaded MPM. A remote attacker could exploit this to cause a denial of service via a specially- crafted cookie. This issue only affected Ubuntu 11.04 and 11.10. (CVE-2012-0021)
It was discovered that the Apache HTTP Server incorrectly handled certain type fields within a scoreboard shared memory segment. A local attacker could exploit this to to cause a denial of service.
(CVE-2012-0031)
Norman Hippert discovered that the Apache HTTP Server incorrecly handled header information when returning a Bad Request (400) error page. A remote attacker could exploit this to obtain the values of certain HTTPOnly cookies.
(CVE-2012-0053)

See Also

http://www.ubuntu.com/usn/usn-1368-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-2011-3607
CVE	CVE-2011-4317
CVE	CVE-2012-0021
CVE	CVE-2012-0031
CVE	CVE-2012-0053
XREF	USN:1368-1
XREF	IAVA:2012-A-0017

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : apache2.2-common_2.2.14-5ubuntu8.4
    Fixed package     : apache2.2-common_2.2.14-5ubuntu8.8
```

30218 (1) - Terminal Services Encryption Level is not FIPS-140 Compliant

Synopsis

The remote host is not FIPS-140 compliant.

Description

The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.

Solution

Change RDP encryption level to :
4. FIPS Compliant

Risk Factor

Low

CVSS Base Score

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

Hosts

192.168.1.16 (tcp/3389)

```
The terminal services encryption level is set to :

2. Medium (Client Compatible)
```

42880 (1) - 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://extendedsubset.com/?p=8

http://www.ietf.org/mail-archive/web/tls/current/msg03948.html

http://www.kb.cert.org/vuls/id/120541

http://www.g-sec.lu/practicaltls.pdf

http://tools.ietf.org/html/rfc5746

Solution

Contact the vendor for specific patch information.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	36935
CVE	CVE-2009-3555
XREF	OSVDB:59968
XREF	OSVDB:59969
XREF	OSVDB:59970
XREF	OSVDB:59971
XREF	OSVDB:59972
XREF	OSVDB:59973
XREF	OSVDB:59974
XREF	OSVDB:60366
XREF	OSVDB:60521
XREF	OSVDB:61234
XREF	OSVDB:61718
XREF	OSVDB:61784

XREF	OSVDB:61785
XREF	OSVDB:61929
XREF	OSVDB:62064
XREF	OSVDB:62135
XREF	OSVDB:62210
XREF	OSVDB:62273
XREF	OSVDB:62536
XREF	OSVDB:62877
XREF	OSVDB:64040
XREF	OSVDB:64499
XREF	OSVDB:64725
XREF	OSVDB:65202
XREF	OSVDB:66315
XREF	OSVDB:67029
XREF	OSVDB:69032
XREF	OSVDB:69561
XREF	OSVDB:70055
XREF	OSVDB:70620
XREF	OSVDB:71951
XREF	OSVDB:71961
XREF	OSVDB:74335
XREF	OSVDB:75622
XREF	OSVDB:77832
XREF	IAVA:2009-A-0122
XREF	IAVA:2010-A-0047
XREF	IAVA:2010-A-0048
XREF	IAVA:2010-A-0072
XREF	IAVA:2010-A-0089
XREF	IAVA:2010-A-0108
XREF	IAVA:2010-A-0149
XREF	IAVA:2010-A-0155

XREF	IAVA:2011-A-0007
XREF	IAVA:2011-A-0055
XREF	IAVA:2011-A-0058
XREF	IAVA:2011-A-0107
XREF	CWE:310

Hosts

192.168.1.81 (tcp/443)

```
Port 443 supports insecure renegotiation over TLSv1.
```

50686 (1) - IP Forwarding Enabled

Synopsis

The remote host has IP forwarding enabled.

Description

The remote host has IP forwarding enabled. An attacker may use this flaw to use the to route packets through this host and potentially bypass some firewalls / routers / NAC filtering.
Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :
echo 0 > /proc/sys/net/ipv4/ip_forward
On Windows, set the key 'IPEnableRouter' to 0 under
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameter
On Mac OS X, you can disable IP forwarding by executing the command :
sysctl -w net.inet.ip.forwarding=0
For other systems, check with your vendor.

Risk Factor

Low

CVSS Base Score

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

References

CVE	CVE-1999-0511

Hosts

192.168.1.208 (tcp/0)

53491 (1) - SSL / TLS Renegotiation DoS

Synopsis

The remote service allows repeated renegotiation of TLS / SSL connections.

Description

The remote service encrypts traffic using TLS / SSL and permits clients to renegotiate connections. The computational requirements for renegotiating a connection are asymmetrical between the client and the server, with the server performing several times more work. Since the remote host does not appear to limit the number of renegotiations for a single TLS / SSL connection, this permits a client to open several simultaneous connections and repeatedly renegotiate them, possibly leading to a denial of service condition.

See Also

http://orchilles.com/2011/03/ssl-renegotiation-dos.html

http://www.ietf.org/mail-archive/web/tls/current/msg07553.html

Solution

Contact the vendor for specific patch information.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	48626
CVE	CVE-2011-1473
XREF	OSVDB:73894

Hosts

192.168.1.13 (tcp/1243)

```
Port 1243 is vulnerable to renegotiation DoS over TLSv1.
```

55099 (1) - USN-1138-1 : dbus-glib vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that DBus-GLib did not properly verify the access flag of exported GObject properties under certain circumstances. A local attacker could exploit this to bypass intended access restrictions or possibly cause a denial of service.

See Also

http://www.ubuntu.com/usn/usn-1138-1/

Solution

Update the affected package(s).

Risk Factor

Low

CVSS Base Score

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

References

CVE	CVE-2010-1172
XREF	USN:1138-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : libdbus-glib-1-2_0.84-1
    Fixed package     : libdbus-glib-1-2_0.84-1ubuntu0.2
```

56389 (1) - USN-1226-1 : samba vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Dan Rosenberg discovered that Samba incorrectly handled changes to the mtab file. A local attacker could use this issue to corrupt the mtab file, possibly leading to a denial of service. (CVE-2011-1678)
Jan Lieskovsky discovered that Samba incorrectly filtered certain strings being added to the mtab file. A local attacker could use this issue to corrupt the mtab file, possibly leading to a denial of service. This issue only affected Ubuntu 10.04 LTS. (CVE-2011-2724)
Dan Rosenberg discovered that Samba incorrectly handled the mtab lock file. A local attacker could use this issue to create a stale lock file, possibly leading to a denial of service. (CVE-2011-3585)

See Also

http://www.ubuntu.com/usn/usn-1226-1/

Solution

Update the affected package(s).

Risk Factor

Low

CVSS Base Score

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

References

CVE	CVE-2011-1678
CVE	CVE-2011-2724
CVE	CVE-2011-3585
XREF	USN:1226-1

Hosts

192.168.1.248 (tcp/0)

```
  - Installed package : smbfs_2:3.4.7~dfsg-1ubuntu3.6
    Fixed package     : smbfs_2:3.4.7~dfsg-1ubuntu3.8
```

11219 (51) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Hosts

192.168.1.1 (tcp/21)

```
Port 21/tcp was found to be open
```

192.168.1.1 (tcp/22)

```
Port 22/tcp was found to be open
```

192.168.1.1 (tcp/80)

```
Port 80/tcp was found to be open
```

192.168.1.10 (tcp/22)

```
Port 22/tcp was found to be open
```

192.168.1.10 (tcp/53)

```
Port 53/tcp was found to be open
```

192.168.1.13 (tcp/22)

```
Port 22/tcp was found to be open
```

192.168.1.13 (tcp/111)

```
Port 111/tcp was found to be open
```

192.168.1.13 (tcp/664)

```
Port 664/tcp was found to be open
```

192.168.1.13 (tcp/1243)

```
Port 1243/tcp was found to be open
```

192.168.1.16 (tcp/135)

```
Port 135/tcp was found to be open
```

192.168.1.16 (tcp/445)

```
Port 445/tcp was found to be open
```

192.168.1.16 (tcp/554)

```
Port 554/tcp was found to be open
```

192.168.1.16 (tcp/912)

```
Port 912/tcp was found to be open
```

192.168.1.16 (tcp/2869)

```
Port 2869/tcp was found to be open
```

192.168.1.16 (tcp/3389)

```
Port 3389/tcp was found to be open
```

192.168.1.30 (tcp/80)

```
Port 80/tcp was found to be open
```

192.168.1.30 (tcp/111)

```
Port 111/tcp was found to be open
```

192.168.1.30 (tcp/139)

```
Port 139/tcp was found to be open
```

192.168.1.30 (tcp/443)

```
Port 443/tcp was found to be open
```

192.168.1.30 (tcp/445)

```
Port 445/tcp was found to be open
```

192.168.1.30 (tcp/548)

```
Port 548/tcp was found to be open
```

192.168.1.30 (tcp/631)

```
Port 631/tcp was found to be open
```

192.168.1.30 (tcp/2049)

```
Port 2049/tcp was found to be open
```

192.168.1.78 (tcp/53)

```
Port 53/tcp was found to be open
```

192.168.1.78 (tcp/80)

```
Port 80/tcp was found to be open
```

192.168.1.78 (tcp/8000)

```
Port 8000/tcp was found to be open
```

192.168.1.79 (tcp/53)

```
Port 53/tcp was found to be open
```

192.168.1.79 (tcp/80)

```
Port 80/tcp was found to be open
```

192.168.1.79 (tcp/8000)

```
Port 8000/tcp was found to be open
```

192.168.1.80 (tcp/80)

```
Port 80/tcp was found to be open
```

192.168.1.80 (tcp/1111)

```
Port 1111/tcp was found to be open
```

192.168.1.81 (tcp/80)

```
Port 80/tcp was found to be open
```

192.168.1.81 (tcp/443)

```
Port 443/tcp was found to be open
```

192.168.1.81 (tcp/1390)

```
Port 1390/tcp was found to be open
```

192.168.1.81 (tcp/1393)

```
Port 1393/tcp was found to be open
```

192.168.1.81 (tcp/1400)

```
Port 1400/tcp was found to be open
```

192.168.1.81 (tcp/1410)

```
Port 1410/tcp was found to be open
```

192.168.1.81 (tcp/1413)

```
Port 1413/tcp was found to be open
```

192.168.1.81 (tcp/2190)

```
Port 2190/tcp was found to be open
```

192.168.1.81 (tcp/2191)

```
Port 2191/tcp was found to be open
```

192.168.1.200 (tcp/8060)

```
Port 8060/tcp was found to be open
```

192.168.1.200 (tcp/8080)

```
Port 8080/tcp was found to be open
```

192.168.1.200 (tcp/8887)

```
Port 8887/tcp was found to be open
```

192.168.1.211 (tcp/3689)

```
Port 3689/tcp was found to be open
```

192.168.1.213 (tcp/8060)

```
Port 8060/tcp was found to be open
```

192.168.1.213 (tcp/8080)

```
Port 8080/tcp was found to be open
```

192.168.1.213 (tcp/8887)

```
Port 8887/tcp was found to be open
```

192.168.1.231 (tcp/22)

```
Port 22/tcp was found to be open
```

192.168.1.231 (tcp/1241)

```
Port 1241/tcp was found to be open
```

192.168.1.231 (tcp/3689)

```
Port 3689/tcp was found to be open
```

192.168.1.231 (tcp/8834)

```
Port 8834/tcp was found to be open
```

22964 (31) - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible 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

Hosts

192.168.1.1 (tcp/22)

```
An SSH server is running on this port.
```

192.168.1.1 (tcp/80)

```
A web server is running on this port.
```

192.168.1.10 (tcp/22)

```
An SSH server is running on this port.
```

192.168.1.13 (tcp/22)

```
An SSH server is running on this port.
```

192.168.1.13 (tcp/1243)

```
A TLSv1 server answered on this port.
```

192.168.1.16 (tcp/912)

```
A VMware authentication daemon is running on this port.
```

192.168.1.30 (tcp/80)

```
A web server is running on this port.
```

192.168.1.30 (tcp/443)

```
A TLSv1 server answered on this port.
```

192.168.1.30 (tcp/443)

```
A web server is running on this port through TLSv1.
```

192.168.1.30 (tcp/631)

```
A web server is running on this port.
```

192.168.1.78 (tcp/80)

```
A web server is running on this port.
```

192.168.1.78 (tcp/8000)

```
A web server is running on this port.
```

192.168.1.79 (tcp/80)

```
A web server is running on this port.
```

192.168.1.79 (tcp/8000)

```
A web server is running on this port.
```

192.168.1.80 (tcp/80)

```
A web server is running on this port.
```

192.168.1.81 (tcp/80)

```
A web server is running on this port.
```

192.168.1.81 (tcp/443)

```
A TLSv1 server answered on this port.
```

192.168.1.81 (tcp/443)

```
A web server is running on this port through TLSv1.
```

192.168.1.81 (tcp/1390)

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

192.168.1.81 (tcp/1393)

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

192.168.1.81 (tcp/1400)

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

192.168.1.81 (tcp/1410)

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

192.168.1.81 (tcp/1413)

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

192.168.1.200 (tcp/8060)

```
A web server is running on this port.
```

192.168.1.211 (tcp/3689)

```
A web server is running on this port.
```

192.168.1.213 (tcp/8060)

```
A web server is running on this port.
```

192.168.1.231 (tcp/22)

```
An SSH server is running on this port.
```

192.168.1.231 (tcp/1241)

```
A TLSv1 server answered on this port.
```

192.168.1.231 (tcp/3689)

```
A web server is running on this port.
```

192.168.1.231 (tcp/8834)

```
A TLSv1 server answered on this port.
```

192.168.1.231 (tcp/8834)

```
A web server is running on this port through TLSv1.
```

19506 (17) - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of plugin feed (HomeFeed or ProfessionalFeed)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- 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

Hosts

192.168.1.1 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Scan Start Date : 2012/3/21 8:26
Scan duration : 333 sec
```

192.168.1.10 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
```

```
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Scan Start Date : 2012/3/21 8:26
Scan duration : 77 sec
```

192.168.1.13 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Scan Start Date : 2012/3/21 8:26
Scan duration : 75 sec
```

192.168.1.16 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/3/21 8:26
Scan duration : 737 sec
```

192.168.1.30 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
```

```
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/3/21 8:26
Scan duration : 2431 sec
```

192.168.1.78 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/3/21 8:26
Scan duration : 1385 sec
```

192.168.1.79 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/3/21 8:26
Scan duration : 1557 sec
```

192.168.1.80 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
```

```
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/3/21 8:26
Scan duration : 174 sec
```

192.168.1.81 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/3/21 8:26
Scan duration : 390 sec
```

192.168.1.85 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/3/21 8:26
Scan duration : 244 sec
```

192.168.1.200 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
```

```
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/3/21 8:26
Scan duration : 488 sec
```

192.168.1.208 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/3/21 8:26
Scan duration : 146 sec
```

192.168.1.211 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/3/21 8:26
Scan duration : 980 sec
```

192.168.1.213 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248
```

```
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/3/21 8:26
Scan duration : 106 sec
```

192.168.1.231 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Scan Start Date : 2012/3/21 8:26
Scan duration : 281 sec
```

192.168.1.245 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248

WARNING : no port scanner was enabled during the scan. This may
lead to incomplete results

Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/3/21 8:26
Scan duration : 13 sec
```

192.168.1.248 (tcp/0)

```
Information about this scan :

Nessus version : 5.0.0
Plugin feed version : 201203131335
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.248

WARNING : no port scanner was enabled during the scan. This may
lead to incomplete results

Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Scan Start Date : 2012/3/21 8:26
Scan duration : 54 sec
```

35716 (15) - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be deduced from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit 'Organizationally Unique Identifier'.
These OUI are registered by IEEE.

See Also

http://standards.ieee.org/faqs/OUI.html

http://standards.ieee.org/regauth/oui/index.shtml

Solution

n/a

Risk Factor

None

Hosts

192.168.1.1 (tcp/0)

```
The following card manufacturers were identified :

00:0d:b9:1c:0e:35 : PC Engines GmbH
```

192.168.1.10 (tcp/0)

```
The following card manufacturers were identified :

00:00:24:c9:55:21 : CONNECT AS
```

192.168.1.13 (tcp/0)

```
The following card manufacturers were identified :

00:a0:cc:3d:b3:ba : LITE-ON COMMUNICATIONS, INC.
```

192.168.1.16 (tcp/0)

```
The following card manufacturers were identified :

00:24:1d:52:d4:fb : GIGA-BYTE TECHNOLOGY CO.,LTD.
```

192.168.1.30 (tcp/0)

```
The following card manufacturers were identified :

00:0d:a2:01:83:fb : Infrant Technologies, Inc.
```

192.168.1.78 (tcp/0)

```
The following card manufacturers were identified :

00:0d:b9:24:2b:d8 : PC Engines GmbH
```

192.168.1.79 (tcp/0)

```
The following card manufacturers were identified :

00:0d:b9:24:2b:d8 : PC Engines GmbH
```

192.168.1.80 (tcp/0)

```
The following card manufacturers were identified :

00:25:9c:8f:80:dd : Cisco-Linksys, LLC
```

192.168.1.81 (tcp/0)

```
The following card manufacturers were identified :

00:25:9c:8f:80:dd : Cisco-Linksys, LLC
```

192.168.1.85 (tcp/0)

```
The following card manufacturers were identified :

7c:2e:0d:00:3e:9f : Blackmagic Design
```

192.168.1.200 (tcp/0)

```
The following card manufacturers were identified :

00:0d:4b:ac:7c:59 : Roku, LLC
```

192.168.1.208 (tcp/0)

```
The following card manufacturers were identified :

00:26:99:48:4d:4a : Cisco Systems
```

192.168.1.211 (tcp/0)

```
The following card manufacturers were identified :

00:1b:63:f0:78:d1 : Apple Computer Inc.
```

192.168.1.213 (tcp/0)

```
The following card manufacturers were identified :

00:0d:4b:4c:29:5e : Roku, LLC
```

192.168.1.231 (tcp/0)

```
The following card manufacturers were identified :

3c:07:54:40:7f:a0 : Apple, Inc.
```

10287 (14) - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.1 (udp/0)

```
For your information, here is the traceroute from 192.168.1.248 to 192.168.1.1 :
192.168.1.248
192.168.1.1
```

192.168.1.10 (udp/0)

```
For your information, here is the traceroute from 192.168.1.248 to 192.168.1.10 :
192.168.1.248
192.168.1.10
```

192.168.1.13 (udp/0)

```
For your information, here is the traceroute from 192.168.1.248 to 192.168.1.13 :
192.168.1.248
192.168.1.13
```

192.168.1.16 (udp/0)

```
For your information, here is the traceroute from 192.168.1.248 to 192.168.1.16 :
192.168.1.248
192.168.1.16
```

192.168.1.30 (udp/0)

```
For your information, here is the traceroute from 192.168.1.248 to 192.168.1.30 :
192.168.1.248
192.168.1.30
```

192.168.1.78 (udp/0)

```
For your information, here is the traceroute from 192.168.1.248 to 192.168.1.78 :
192.168.1.248
192.168.1.78
```

192.168.1.79 (udp/0)

```
For your information, here is the traceroute from 192.168.1.248 to 192.168.1.79 :
192.168.1.248
192.168.1.79
```

192.168.1.80 (udp/0)

```
For your information, here is the traceroute from 192.168.1.248 to 192.168.1.80 :
192.168.1.248
192.168.1.80
```

192.168.1.81 (udp/0)

```
For your information, here is the traceroute from 192.168.1.248 to 192.168.1.81 :
192.168.1.248
192.168.1.81
```

192.168.1.85 (udp/0)

```
For your information, here is the traceroute from 192.168.1.248 to 192.168.1.85 :
192.168.1.248
192.168.1.85
```

192.168.1.200 (udp/0)

```
For your information, here is the traceroute from 192.168.1.248 to 192.168.1.200 :
192.168.1.248
```

```
192.168.1.200
```

192.168.1.211 (udp/0)

```
For your information, here is the traceroute from 192.168.1.248 to 192.168.1.211 :
192.168.1.248
192.168.1.211
```

192.168.1.213 (udp/0)

```
For your information, here is the traceroute from 192.168.1.248 to 192.168.1.213 :
192.168.1.248
192.168.1.213
```

192.168.1.231 (udp/0)

```
For your information, here is the traceroute from 192.168.1.248 to 192.168.1.231 :
192.168.1.248
192.168.1.231
```

11111 (14) - 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

Hosts

192.168.1.13 (tcp/111)

```

The following RPC services are available on TCP port 111 :

 - program: 100000 (portmapper), version: 2
```

192.168.1.13 (udp/111)

```

The following RPC services are available on UDP port 111 :

 - program: 100000 (portmapper), version: 2
```

192.168.1.13 (udp/661)

```

The following RPC services are available on UDP port 661 :

 - program: 100024 (status), version: 1
```

192.168.1.13 (tcp/664)

```

The following RPC services are available on TCP port 664 :

 - program: 100024 (status), version: 1
```

192.168.1.30 (tcp/111)

```

The following RPC services are available on TCP port 111 :

 - program: 100000 (portmapper), version: 2
```

192.168.1.30 (udp/111)

```

The following RPC services are available on UDP port 111 :

 - program: 100000 (portmapper), version: 2
```

192.168.1.30 (tcp/2049)

```

The following RPC services are available on TCP port 2049 :

 - program: 100003 (nfs), version: 2
 - program: 100003 (nfs), version: 3
 - program: 100003 (nfs), version: 4
```

192.168.1.30 (udp/2049)

```

The following RPC services are available on UDP port 2049 :

 - program: 100003 (nfs), version: 2
 - program: 100003 (nfs), version: 3
 - program: 100003 (nfs), version: 4
```

192.168.1.30 (udp/3130)

```
The following RPC services are available on UDP port 3130 :

 - program: 100021 (nlockmgr), version: 1
 - program: 100021 (nlockmgr), version: 3
 - program: 100021 (nlockmgr), version: 4
```

192.168.1.30 (udp/3131)

```
The following RPC services are available on UDP port 3131 :

 - program: 100005 (mountd), version: 1
 - program: 100005 (mountd), version: 2
 - program: 100005 (mountd), version: 3
```

192.168.1.30 (tcp/4181)

```
The following RPC services are available on TCP port 4181 :

 - program: 100005 (mountd), version: 1
 - program: 100005 (mountd), version: 2
 - program: 100005 (mountd), version: 3
```

192.168.1.30 (tcp/4955)

```
The following RPC services are available on TCP port 4955 :

 - program: 100021 (nlockmgr), version: 1
 - program: 100021 (nlockmgr), version: 3
 - program: 100021 (nlockmgr), version: 4
```

192.168.1.30 (tcp/32765)

```
The following RPC services are available on TCP port 32765 :

 - program: 100024 (status), version: 1
```

192.168.1.30 (udp/32765)

```
The following RPC services are available on UDP port 32765 :

 - program: 100024 (status), version: 1
```

11936 (14) - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes, (TCP/IP, SMB, HTTP, NTP, SNMP, etc...) it is possible to guess the name of the remote operating system in use, and sometimes its version.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.1 (tcp/0)

```
Remote operating system : FreeBSD 7.3
FreeBSD 7.4
Confidence Level : 85
Method : SSH


The remote host is running one of these operating systems :
FreeBSD 7.3
FreeBSD 7.4
```

192.168.1.10 (tcp/0)

```
Remote operating system : Linux Kernel 2.6 on Debian 5.0 (lenny)
Confidence Level : 95
Method : SSH


The remote host is running Linux Kernel 2.6 on Debian 5.0 (lenny)
```

192.168.1.13 (tcp/0)

```
Remote operating system : Linux Kernel 2.6
Confidence Level : 65
Method : SinFP


The remote host is running Linux Kernel 2.6
```

192.168.1.16 (tcp/0)

```
Remote operating system : Windows 7 Ultimate
Confidence Level : 69
Method : MSRPC


The remote host is running Windows 7 Ultimate
```

192.168.1.30 (tcp/0)

```
Remote operating system : Linux Kernel 2.4
Linux Kernel 2.6
Confidence Level : 54
Method : SinFP


The remote host is running one of these operating systems :
Linux Kernel 2.4
Linux Kernel 2.6
```

192.168.1.78 (tcp/0)

```
Remote operating system : Microsoft Windows Vista
```

```
Confidence Level : 65
Method : SinFP


The remote host is running Microsoft Windows Vista
```

192.168.1.79 (tcp/0)

```
Remote operating system : Microsoft Windows Vista
Confidence Level : 65
Method : SinFP


The remote host is running Microsoft Windows Vista
```

192.168.1.80 (tcp/0)

```
Remote operating system : Linksys Wireless Access Point - WET610N
Confidence Level : 95
Method : HNAP


The remote host is running Linksys Wireless Access Point - WET610N
```

192.168.1.81 (tcp/0)

```
Remote operating system : Linux Kernel 2.6
Confidence Level : 70
Method : SinFP


The remote host is running Linux Kernel 2.6
```

192.168.1.200 (tcp/0)

```
Remote operating system : Cyber Switching ePower PDU
Confidence Level : 70
Method : SinFP


The remote host is running Cyber Switching ePower PDU
```

192.168.1.211 (tcp/0)

```
Remote operating system : AppleTV/3.0
Confidence Level : 98
Method : NTP


The remote host is running AppleTV/3.0
```

192.168.1.213 (tcp/0)

```
Remote operating system : Cyber Switching ePower PDU
Confidence Level : 70
Method : SinFP


The remote host is running Cyber Switching ePower PDU
```

192.168.1.231 (tcp/0)

```
Remote operating system : Mac OS X 10.7
iOS 4
Confidence Level : 59
Method : SinFP


The remote host is running one of these operating systems :
Mac OS X 10.7
iOS 4
```

192.168.1.248 (tcp/0)

```
Remote operating system : Linux Kernel 2.6.39.4 on Ubuntu 10.04
Confidence Level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 2.6.39.4 on Ubuntu 10.04
```

10114 (13) - 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.
This may help an attacker to defeat all time-based authentication protocols.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Hosts

192.168.1.1 (icmp/0)

```
The remote clock is synchronized with the local clock.
```

192.168.1.10 (icmp/0)

```
The difference between the local and remote clocks is 5489 seconds.
```

192.168.1.13 (icmp/0)

```
The difference between the local and remote clocks is 1317 seconds.
```

192.168.1.16 (icmp/0)

```
This host returns non-standard timestamps (high bit is set)
The ICMP timestamps might be in little endian format (not in network format)
The difference between the local and remote clocks is -489 seconds.
```

192.168.1.30 (icmp/0)

```
The remote clock is synchronized with the local clock.
```

192.168.1.78 (icmp/0)

```
The difference between the local and remote clocks is 8733 seconds.
```

192.168.1.79 (icmp/0)

```
The difference between the local and remote clocks is 8733 seconds.
```

192.168.1.80 (icmp/0)

```
The difference between the local and remote clocks is 25111 seconds.
```

192.168.1.81 (icmp/0)

```
The difference between the local and remote clocks is 1 second.
```

192.168.1.85 (icmp/0)

```
The difference between the local and remote clocks is 44948 seconds.
```

192.168.1.200 (icmp/0)

```
The difference between the local and remote clocks is 31 seconds.
```

192.168.1.208 (icmp/0)

```
This host returns non-standard timestamps (high bit is set)
```

192.168.1.213 (icmp/0)

```
The difference between the local and remote clocks is -46 seconds.
```

25220 (13) - 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

Hosts

192.168.1.1 (tcp/0)

192.168.1.10 (tcp/0)

192.168.1.13 (tcp/0)

192.168.1.16 (tcp/0)

192.168.1.30 (tcp/0)

192.168.1.78 (tcp/0)

192.168.1.79 (tcp/0)

192.168.1.80 (tcp/0)

192.168.1.81 (tcp/0)

192.168.1.200 (tcp/0)

192.168.1.211 (tcp/0)

192.168.1.213 (tcp/0)

192.168.1.231 (tcp/0)

54615 (13) - 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

Hosts

192.168.1.1 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 85
```

192.168.1.10 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 95
```

192.168.1.13 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 65
```

192.168.1.16 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 69
```

192.168.1.30 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 54
```

192.168.1.78 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 65
```

192.168.1.79 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 65
```

192.168.1.80 (tcp/0)

```
Remote device type : wireless-access-point
Confidence level : 95
```

192.168.1.81 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 70
```

192.168.1.200 (tcp/0)

```
Remote device type : embedded
Confidence level : 70
```

192.168.1.211 (tcp/0)

```
Remote device type : embedded
Confidence level : 98
```

192.168.1.213 (tcp/0)

```
Remote device type : embedded
Confidence level : 70
```

192.168.1.248 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 100
```

24260 (11) - 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 and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.1 (tcp/80)

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : OPTIONS, GET, HEAD, POST
Headers :

  Expires: 0
  Last-Modified: Wed, 21 Mar 2012 12:31:33 GMT
  Cache-Control: no-store, no-cache, must-revalidate
  Cache-Control: post-check=0, pre-check=0
  Pragma: no-cache
  WWW-Authenticate: Basic realm="."
  Content-type: text/html
  Connection: close
  Transfer-Encoding: chunked
  Date: Wed, 21 Mar 2012 12:31:33 GMT
  Server: lighttpd/1.4.23
```

192.168.1.30 (tcp/80)

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : GET,HEAD,POST,OPTIONS,TRACE
Headers :

  Date: Wed, 21 Mar 2012 12:54:56 GMT
  Server: Apache
  Location: http://192.168.1.30/media
  Content-Length: 209
  Keep-Alive: timeout=15, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=iso-8859-1
```

192.168.1.30 (tcp/443)

```
Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : GET,HEAD,POST,OPTIONS,TRACE
Headers :

  Date: Wed, 21 Mar 2012 12:55:29 GMT
  Server: Apache
  Location: https://192.168.1.30/media
  Content-Length: 210
  Keep-Alive: timeout=15, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=iso-8859-1
```

192.168.1.78 (tcp/8000)

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Expires: Tue, 14 Mar 2000 12:20:19 GMT
  Expires: 0
  Cache-Control: max-age=180000
  Cache-Control: no-store, no-cache, must-revalidate
  Cache-Control: post-check=0, pre-check=0
  Pragma: no-cache
  Connection: close
  Content-type: text/html
  Transfer-Encoding: chunked
  Date: Sun, 12 Mar 2000 10:20:28 GMT
  Server: lighttpd/1.4.29
```

192.168.1.79 (tcp/80)

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : OPTIONS, GET, HEAD, POST
Headers :

  Expires: Tue, 14 Mar 2000 12:24:15 GMT
  Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Cache-Control: max-age=180000
  Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
  Pragma: no-cache
  Content-type: text/html
  Connection: close
  Transfer-Encoding: chunked
  Date: Sun, 12 Mar 2000 10:24:22 GMT
  Server: lighttpd/1.4.29
```

192.168.1.79 (tcp/8000)

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Expires: Tue, 14 Mar 2000 12:24:37 GMT
  Expires: 0
  Cache-Control: max-age=180000
  Cache-Control: no-store, no-cache, must-revalidate
  Cache-Control: post-check=0, pre-check=0
  Pragma: no-cache
  Connection: close
  Content-type: text/html
  Transfer-Encoding: chunked
  Date: Sun, 12 Mar 2000 10:24:39 GMT
  Server: lighttpd/1.4.29
```

192.168.1.81 (tcp/80)

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Headers :

  Server: tivo-httpd-1:20.2-01-2:746
  Content-Length: 0
  Location: /index.html
```

```
    Connection: keep-alive
    Keep-Alive: max=10, timeout=30
```

192.168.1.81 (tcp/443)

```
  Protocol version : HTTP/1.1
  SSL : yes
  Keep-Alive : yes
  Headers :

    Server: tivo-httpd-1:20.2-01-2:746
    WWW-Authenticate: Digest realm="TiVo DVR", nonce="BE3C4BDE078ACF84", qop="auth"
    Content-Length: 31
    Content-Type: text/html
    Connection: keep-alive
    Keep-Alive: max=10, timeout=30
```

192.168.1.211 (tcp/3689)

```
  Protocol version : HTTP/1.1
  SSL : no
  Keep-Alive : no
  Options allowed : (Not implemented)
  Headers :

    Date: Wed, 21 Mar 2012 12:41:30 GMT
    RIPT-Server: iTunesLib/3.0.2 (Mac OS X)
    Content-Type: application/x-dmap-tagged
    Content-Length: 0
```

192.168.1.231 (tcp/8834)

```
  Protocol version : HTTP/1.1
  SSL : yes
  Keep-Alive : no
  Options allowed : (Not implemented)
  Headers :

    Date: Wed, 21 Mar 2012 12:28:28 GMT
    Server: NessusWWW
    Connection: close
    Expires: Wed, 21 Mar 2012 12:28:28 GMT
    Content-Length: 6525
    Content-Type: text/html
    X-Frame-Options: DENY
    Cache-Control:
    Expires: 0
    Pragma :
```

192.168.1.248 (tcp/80)

```
  Protocol version : HTTP/1.1
  SSL : no
  Keep-Alive : yes
  Options allowed : (Not implemented)
  Headers :

    Date: Wed, 21 Mar 2012 12:27:22 GMT
    Server: Apache/2.2.14 (Ubuntu)
    Last-Modified: Tue, 10 May 2011 07:45:00 GMT
    ETag: "493a0-b1-4a2e722183700"
    Accept-Ranges: bytes
    Content-Length: 177
    Vary: Accept-Encoding
    Keep-Alive: timeout=15, max=100
    Connection: Keep-Alive
    Content-Type: text/html
```

45590 (10) - Common Platform Enumeration (CPE)

Synopsis

It is 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/

Solution

n/a

Risk Factor

None

Hosts

192.168.1.1 (tcp/0)

```
The remote operating system matched the following CPE's :

  cpe:/o:freebsd:freebsd:7.3 -> FreeBSD 7.3
  cpe:/o:freebsd:freebsd:7.4 -> FreeBSD 7.4

Following application CPE matched on the remote system :

  cpe:/a:openbsd:openssh:5.1
```

192.168.1.10 (tcp/0)

```
The remote operating system matched the following CPE :

  cpe:/o:debian:debian_linux:5.0 -> Debian GNU/Linux 5.0

Following application CPE's matched on the remote system :

  cpe:/a:openbsd:openssh:5.1
  cpe:/a:isc:bind:Hack
```

192.168.1.13 (tcp/0)

```
The remote operating system matched the following CPE :

  cpe:/o:linux:linux_kernel:2.6

Following application CPE matched on the remote system :

  cpe:/a:openbsd:openssh:4.3 -> OpenBSD OpenSSH 4.3
```

192.168.1.16 (tcp/0)

```
The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_7:::ultimate
```

192.168.1.30 (tcp/0)

```
The remote operating system matched the following CPE's :

  cpe:/o:linux:linux_kernel:2.4
  cpe:/o:linux:linux_kernel:2.6

Following application CPE matched on the remote system :

  cpe:/a:samba:samba:3.0.34 -> Samba 3.0.34
```

192.168.1.78 (tcp/0)

```
The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_vista

Following application CPE matched on the remote system :

  cpe:/a:isc:bind:dnsmasq:2
```

192.168.1.79 (tcp/0)

```
The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_vista

Following application CPE matched on the remote system :

  cpe:/a:isc:bind:dnsmasq:2
```

192.168.1.81 (tcp/0)

```
The remote operating system matched the following CPE :

  cpe:/o:linux:linux_kernel:2.6
```

192.168.1.231 (tcp/0)

```
The remote operating system matched the following CPE :

  cpe:/o:apple:mac_os_x:10.7

Following application CPE matched on the remote system :

  cpe:/a:openbsd:openssh:5.6
```

192.168.1.248 (tcp/0)

```
The remote operating system matched the following CPE :

  cpe:/o:canonical:ubuntu_linux:10.04

Following application CPE matched on the remote system :

  cpe:/a:apache:http_server:2.2.14 -> Apache Software Foundation Apache HTTP Server 2.2.14
```

10107 (9) - 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

Hosts

192.168.1.1 (tcp/80)

```
The remote web server type is :

lighttpd/1.4.23
```

192.168.1.30 (tcp/631)

```
The remote web server type is :

CUPS/1.1
```

192.168.1.78 (tcp/8000)

```
The remote web server type is :

lighttpd/1.4.29
```

192.168.1.80 (tcp/80)

```
The remote web server type is :

GoAhead-Webs
```

192.168.1.81 (tcp/80)

```
The remote web server type is :

tivo-httpd-1:20.2-01-2:746
```

192.168.1.81 (tcp/443)

```
The remote web server type is :

tivo-httpd-1:20.2-01-2:746
```

192.168.1.213 (tcp/8060)

```
The remote web server type is :

Roku UPnP/1.0 MiniUPnPd/1.4
```

192.168.1.231 (tcp/8834)

```
The remote web server type is :

NessusWWW
```

192.168.1.248 (tcp/80)

```
The remote web server type is :

Apache/2.2.14 (Ubuntu)

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.
```

10736 (8) - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) 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/pipe.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.16 (tcp/135)

```
The following DCERPC services are available locally :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0B2410

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0B2410

Object UUID : 6d726574-7273-0076-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Lo [...]
```

192.168.1.16 (tcp/445)

```
The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\O-REN

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\O-REN

Object UUID : 00000000-0000-0000-0000-000000000000
```

```
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\trkwks
Netbios name : \\O-REN

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0767a036-0d22-48aa-ba69-b619480f38cb, version 1.0
Description : Unknown RPC service
Annotation : PcaSvc
Type : Remote RPC service
Named pipe : \pipe\trkwks
Netbios name : \\O-REN

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 123457 [...]
```

192.168.1.16 (tcp/49152)

```
The following DCERPC services are available on TCP port 49152 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49152
IP : 192.168.1.16
```

192.168.1.16 (tcp/49153)

```
The following DCERPC services are available on TCP port 49153 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.1.16

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.1.16

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.1.16

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Remote RPC service
TCP Port :  [...]
```

192.168.1.16 (tcp/49154)

```
The following DCERPC services are available on TCP port 49154 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.1.16
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.1.16

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.1.16

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.1.16

Object UUID : 73736573-6f69-656e-6e7 [...]
```

192.168.1.16 (tcp/49155)

```
The following DCERPC services are available on TCP port 49155 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.1.16
```

192.168.1.16 (tcp/49156)

```
The following DCERPC services are available on TCP port 49156 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.1.16
```

192.168.1.16 (tcp/49157)

```
The following DCERPC services are available on TCP port 49157 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1.0
Description : Unknown RPC service
Annotation : Remote Fw APIs
Type : Remote RPC service
TCP Port : 49157
IP : 192.168.1.16

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Remote RPC service
TCP Port : 49157
IP : 192.168.1.16
```

11002 (6) - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

http://en.wikipedia.org/wiki/Domain_Name_System

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Hosts

192.168.1.10 (tcp/53)
192.168.1.10 (udp/53)
192.168.1.78 (tcp/53)
192.168.1.78 (udp/53)
192.168.1.79 (tcp/53)
192.168.1.79 (udp/53)

10267 (4) - 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

Hosts

192.168.1.1 (tcp/22)

```
SSH version : SSH-2.0-OpenSSH_5.1p1 FreeBSD-20080901
SSH supported authentication : publickey,password,keyboard-interactive
```

192.168.1.10 (tcp/22)

```
SSH version : SSH-2.0-OpenSSH_5.1p1 Debian-5
SSH supported authentication : publickey,password
```

192.168.1.13 (tcp/22)

```
SSH version : SSH-2.0-OpenSSH_4.3
SSH supported authentication : publickey,gssapi-with-mic,password
```

192.168.1.231 (tcp/22)

```
SSH version : SSH-2.0-OpenSSH_5.6
SSH supported authentication : publickey,keyboard-interactive
```

10881 (4) - 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

Hosts

192.168.1.1 (tcp/22)

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0


SSHv2 host key fingerprint : 35:c2:29:c3:67:04:c2:6f:24:64:a0:6a:d8:3c:f2:ab
```

192.168.1.10 (tcp/22)

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0


SSHv2 host key fingerprint : 65:b6:df:e2:a2:2d:8f:7f:c2:f1:83:f6:6f:08:9a:6c
```

192.168.1.13 (tcp/22)

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0


SSHv2 host key fingerprint : 6c:5d:88:93:3f:fa:16:e8:11:b1:0e:19:81:bc:84:46
```

192.168.1.231 (tcp/22)

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0


SSHv2 host key fingerprint : 8b:bc:a5:45:5a:44:3b:6d:3b:d6:17:1c:ee:f7:ff:17
```

21643 (4) - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This script detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

n/a

Risk Factor

None

Hosts

192.168.1.13 (tcp/1243)

```
Here is the list of SSL ciphers supported by the remote server :

  Medium Strength Ciphers (>= 56-bit and < 112-bit key)
    TLSv1
      DES-CBC-SHA                Kx=RSA        Au=RSA     Enc=DES(56)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)
    TLSv1
      DES-CBC3-SHA               Kx=RSA        Au=RSA     Enc=3DES(168)      Mac=SHA1
      AES128-SHA                 Kx=RSA        Au=RSA     Enc=AES(128)       Mac=SHA1
      AES256-SHA                 Kx=RSA        Au=RSA     Enc=AES(256)       Mac=SHA1
      RC4-MD5                    Kx=RSA        Au=RSA     Enc=RC4(128)       Mac=MD5
      RC4-SHA                    Kx=RSA        Au=RSA     Enc=RC4(128)       Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

192.168.1.81 (tcp/443)

```
Here is the list of SSL ciphers supported by the remote server :

  Medium Strength Ciphers (>= 56-bit and < 112-bit key)
    SSLv3
      DES-CBC-SHA                Kx=RSA        Au=RSA     Enc=DES(56)        Mac=SHA1
    TLSv1
      DES-CBC-SHA                Kx=RSA        Au=RSA     Enc=DES(56)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)
    SSLv3
      DES-CBC3-SHA               Kx=RSA        Au=RSA     Enc=3DES(168)      Mac=SHA1
      IDEA-CBC-SHA               Kx=RSA        Au=RSA     Enc=IDEA(128)      Mac=SHA1
      RC4-SHA                    Kx=RSA        Au=RSA     Enc=RC4(128)       Mac=SHA1
    TLSv1
      DES-CBC3-SHA               Kx=RSA        Au=RSA     Enc=3DES(168)      Mac=SHA1
      AES128-SHA                 Kx=RSA        Au=RSA     Enc=AES(128)       Mac=SHA1
      AES256-SHA                 Kx=RSA        Au=RSA     Enc=AES(256)       Mac=SHA1
      IDEA-CBC-SHA               Kx=RSA        Au=RSA     Enc=IDEA(128)      Mac=SHA1
      RC4-SHA       [...]
```

192.168.1.231 (tcp/1241)

```
Here is the list of SSL ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)
```

```
    TLSv1
      DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES(168)        Mac=SHA1
      AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES(128)         Mac=SHA1
      AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES(256)         Mac=SHA1
      RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)         Mac=MD5
      RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)         Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

192.168.1.231 (tcp/8834)

```
Here is the list of SSL ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)
    SSLv3
      DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES(168)        Mac=SHA1
      RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)         Mac=MD5
      RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)         Mac=SHA1
    TLSv1
      DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES(168)        Mac=SHA1
      AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES(128)         Mac=SHA1
      AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES(256)         Mac=SHA1
      RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)         Mac=MD5
      RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)         Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

39520 (4) - 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

http://www.nessus.org/u?d636c8c7

Solution

N/A

Risk Factor

None

Hosts

192.168.1.1 (tcp/22)

```
Give Nessus credentials to perform local checks.
```

192.168.1.10 (tcp/22)

```
Give Nessus credentials to perform local checks.
```

192.168.1.13 (tcp/22)

```
Give Nessus credentials to perform local checks.
```

192.168.1.231 (tcp/22)

```
Give Nessus credentials to perform local checks.
```

56984 (4) - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.13 (tcp/1243)

```
This port supports TLSv1.0.
```

192.168.1.81 (tcp/443)

```
This port supports SSLv2/SSLv3/TLSv1.0.
```

192.168.1.231 (tcp/1241)

```
This port supports TLSv1.0.
```

192.168.1.231 (tcp/8834)

```
This port supports SSLv3/TLSv1.0.
```

10028 (3) - DNS Server BIND version Directive Remote Version Disclosure

Synopsis

It is possible to obtain the version number of the remote DNS server.

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request, for the text 'version.bind' in the domain 'chaos'.
This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of bind by using the 'version' directive in the 'options' section in named.conf

Risk Factor

None

References

XREF	OSVDB:23

Hosts

192.168.1.10 (udp/53)

```

The version of the remote DNS server is :

Hack Naked
```

192.168.1.78 (udp/53)

```

The version of the remote DNS server is :

dnsmasq-2.55
```

192.168.1.79 (udp/53)

```

The version of the remote DNS server is :

dnsmasq-2.55
```

10863 (3) - 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

Hosts

192.168.1.81 (tcp/443)

```
Subject Name:

Common Name: 746-0001-9022-E613
Organization: TiVo Inc.
Organization Unit: IT
Locality: Alviso
State/Province: California
Country: US

Issuer Name:

Common Name: 746-0001-9022-E613
Organization: TiVo Inc.
Organization Unit: IT
Locality: Alviso
State/Province: California
Country: US

Serial Number: 00 DC F2 B1 B4 56 76 02 93

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jan 25 19:07:36 2010 GMT
Not Valid After: Jan 23 19:07:36 2020 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 E6 A5 D7 5B D1 A0 8C 95 65 94 22 CE EA A1 61 96 FD 0E AA
            A4 3E 81 0C B1 0E 42 30 00 F1 40 EC 29 04 02 E7 C8 C5 AA 92
            62 EF E5 A8 C6 F6 F3 59 BA 31 9E 7A C8 A1 74 56 0B 05 65 AD
            AE AB 44 59 AF C1 25 C3 81 D0 34 8D 8E 1E E2 CF 73 EF 04 E9
            AA E3 0D C6 43 40 42 38 6F 60 EF 79 D3 B2 54 61 CD 78 3F 43
            E8 96 73 1C 92 86 C7 0B B4 65 52 E8 F4 6C 3C 16 28 E8 09 80
            0C CD 46 44 09 68 29 3E 61
Exponent: 0 [...]
```

192.168.1.231 (tcp/1241)

```
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: Pauls-MacBook-Pro.local

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
```

```
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 C3 71

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Feb 09 15:01:32 2012 GMT
Not Valid After: Feb 08 15:01:32 2016 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 C9 83 11 F3 D8 F3 1B 14 9F CE AE 2C 8C 0B 68 E4 1E 23 62
            48 3C 9B 79 02 4C A6 E2 F0 47 45 E1 C8 E3 F6 B3 BA 33 C4 71
            74 F9 B8 00 A5 6F 4D BA 56 43 A4 38 79 61 E2 57 E6 B1 7F 7B
            6F BE 6E 95 15 97 67 D3 49 C3 90 63 47 A9 BF 9B 44 83 53 52
            00 10 6D 89 CC 8F F6 BA 3A 3B 09 FA 15 63 0A C0 17 A6 33 40
            AB 29 1C 7A C6 62 48 A6 E3 2F 27 26 49 B3 D0 47 2E 4C A6 6E
      [...]
```

192.168.1.231 (tcp/8834)

```
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: Pauls-MacBook-Pro.local

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 C3 71

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Feb 09 15:01:32 2012 GMT
Not Valid After: Feb 08 15:01:32 2016 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 C9 83 11 F3 D8 F3 1B 14 9F CE AE 2C 8C 0B 68 E4 1E 23 62
            48 3C 9B 79 02 4C A6 E2 F0 47 45 E1 C8 E3 F6 B3 BA 33 C4 71
            74 F9 B8 00 A5 6F 4D BA 56 43 A4 38 79 61 E2 57 E6 B1 7F 7B
            6F BE 6E 95 15 97 67 D3 49 C3 90 63 47 A9 BF 9B 44 83 53 52
            00 10 6D 89 CC 8F F6 BA 3A 3B 09 FA 15 63 0A C0 17 A6 33 40
            AB 29 1C 7A C6 62 48 A6 E3 2F 27 26 49 B3 D0 47 2E 4C A6 6E
      [...]
```

11011 (3) - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.16 (tcp/445)

```
A CIFS server is running on this port.
```

192.168.1.30 (tcp/139)

```
An SMB server is running on this port.
```

192.168.1.30 (tcp/445)

```
A CIFS server is running on this port.
```

35371 (3) - DNS Server hostname.bind Map Hostname Disclosure

Synopsis

The DNS server discloses the remote host name.

Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

Risk Factor

None

Hosts

192.168.1.10 (udp/53)

```
The remote host name is :

madmonk
```

192.168.1.78 (udp/53)

```
The remote host name is :

madmonk
```

192.168.1.79 (udp/53)

```
The remote host name is :

madmonk
```

35373 (3) - DNS Server DNSSEC Aware Resolver

Synopsis

The remote DNS resolver is DNSSEC-aware.

Description

The remote DNS resolver accepts DNSSEC options. This means that it may verify the authenticity of DNSSEC protected zones if it is configured to trust their keys.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.10 (udp/53)

192.168.1.78 (udp/53)

192.168.1.79 (udp/53)

10150 (2) - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It is possible to obtain the network name of the remote host.

Description

The remote host listens on UDP port 137 or TCP port 445 and replies to NetBIOS nbtscan or SMB requests.
Note that this plugin gathers information to be used in other plugins but does not itself generate a report.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.30 (udp/137)

```
The following 7 NetBIOS names have been gathered :

 NAS-BASEMENT      = Computer name
 NAS-BASEMENT      = Messenger Service
 NAS-BASEMENT      = File Server Service
 __MSBROWSE__      = Master Browser
 PAULDOTCOM        = Master Browser
 PAULDOTCOM        = Browser Service Elections
 PAULDOTCOM        = Workgroup / Domain name

This SMB server seems to be a SAMBA server (MAC address is NULL).
```

192.168.1.231 (udp/137)

```
The following 1 NetBIOS names have been gathered :

 MACBOOKPRO-7FA0  = Computer name

The remote host has the following MAC address on its adapter :
   3c:07:54:40:7f:a0
```

10223 (2) - 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

References

CVE	CVE-1999-0632

Hosts

192.168.1.13 (udp/111)

192.168.1.30 (udp/111)

10394 (2) - Microsoft Windows SMB Log In Possible

Synopsis

It is possible to log into the remote host.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Exploitable with

Metasploit (true)

Hosts

192.168.1.16 (tcp/445)

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

192.168.1.30 (tcp/445)

```
- NULL sessions are enabled on the remote host
- Remote users are authenticated as 'Guest'
```

10397 (2) - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

Synopsis

It is possible to obtain network information.

Description

It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe.
The browse list is the list of the nearest Windows systems of the remote host.

Solution

n/a

Risk Factor

None

References

XREF	OSVDB:300

Hosts

192.168.1.16 (tcp/445)

```
Here is the browse list of the remote host :

O-REN ( os : 6.1 )
```

192.168.1.30 (tcp/445)

```
Here is the browse list of the remote host :

NAS-BASEMENT ( os : 0.0 )
```

10785 (2) - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It is possible to obtain information about the remote operating system.

Description

It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.16 (tcp/445)

```
The remote Operating System is : Windows 7 Ultimate 7601 Service Pack 1
The remote native lan manager is : Windows 7 Ultimate 6.1
The remote SMB Domain Name is : O-REN
```

192.168.1.30 (tcp/445)

```
The remote Operating System is : Unix
The remote native lan manager is : Samba 3.0.34
The remote SMB Domain Name is : PAULDOTCOM
```

10884 (2) - Network Time Protocol (NTP) Server Detection

Synopsis

An NTP server is listening on the remote host.

Description

An NTP (Network Time Protocol) server is listening on this port. It provides information about the current date and time of the remote system and may provide system information.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.211 (udp/123)

```
It was possible to gather the following information from the remote NTP host :

version='ntpd 4.2.0@1.1161-r Sat Oct  7 04:38:28 PDT 2006 (1)',
processor='i386', system='Darwin/8.8.2', leap=3, stratum=16,
precision=-20, rootdelay=0.000, rootdispersion=25948.785, peer=0,
refid=INIT, reftime=0x00000000.00000000, poll=4,
clock=0xd3144ae8.e210f0e9, state=0, offset=0.000, frequency=0.000,
jitter=0.001, stability=0.000
```

192.168.1.231 (udp/123)

43111 (2) - 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.
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.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.30 (tcp/631)

```
Based on the response to an OPTIONS request :

  - HTTP methods  HEAD  OPTIONS  POST  PUT GET are allowed on :

    /
```

192.168.1.248 (tcp/80)

```
Based on the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
```

53335 (2) - 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

Hosts

192.168.1.13 (tcp/111)
192.168.1.30 (tcp/111)

10147 (1) - Nessus Server Detection

Synopsis

A Nessus daemon is listening on the remote port.

Description

A Nessus daemon is listening on the remote port. It is not recommended to let anyone connect to this port.
Also, make sure that the remote Nessus installation has been authorized.

Solution

Filter incoming traffic to this port.

Risk Factor

None

Hosts

192.168.1.231 (tcp/1241)

10386 (1) - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.
Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.78 (tcp/8000)

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 302
rather than 404. The requested URL was :

    http://192.168.1.78:8000/PcFT41Iadusu.html
```

10395 (1) - Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

N/A

Risk Factor

None

Hosts

192.168.1.30 (tcp/445)

```
Here are the SMB shares available on the remote host when logged as oheshmid:

  - IPC$
  - media
  - backup
```

10437 (1) - NFS Share Export List

Synopsis

The remote NFS server exports a list of shares.

Description

This plugin retrieves the list of NFS exported shares.

See Also

http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

Solution

Ensure each share is intended to be exported.

Risk Factor

None

Hosts

192.168.1.30 (tcp/2049)

```
Here is the export list of 192.168.1.30 :

/c/media *
/c/backup *
```

10666 (1) - Apple Filing Protocol Server Detection

Synopsis

An Apple file sharing service is listening on the remote port.

Description

The remote service understands the Apple Filing Protocol (AFP) and responds to a 'FPGetSrvrInfo' ('DSIGetStatus') request with information about itself.
AFP is used to offer file services for Mac OS X as well as the older Mac OS. In the past, it has also been known as 'AppleTalk Filing Protocol' and 'AppleShare'.

See Also

http://www.nessus.org/u?7cadff1c

http://en.wikipedia.org/wiki/Apple_Filing_Protocol

Solution

n/a

Risk Factor

None

Hosts

192.168.1.30 (tcp/548)

```
Nessus collected the following information about the remote AFP service :

  Server name  : NAS-BASEMENT
  Machine type : Netatalk
  UAMs         : No User Authent, DHCAST128, Cleartxt Passwrd
  AFP versions : AFPVersion 1.1, AFPVersion 2.0, AFPVersion 2.1, AFP2.2, AFPX03, AFP3.1, AFP3.2


The server allows the "guest" user to connect.
```

10859 (1) - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Hosts

192.168.1.30 (tcp/445)

```
The remote host SID value is :

1-5-21-3581115777-3128578739-639081464

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

10860 (1) - SMB Use Host SID to Enumerate Local Users

Synopsis

It is possible to enumerate local users.

Description

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

Solution

n/a

Risk Factor

None

Hosts

192.168.1.30 (tcp/445)

```
  - nobody (id 501, Guest account)
  - admin (id 1196)

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

10919 (1) - Open Port Re-check

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.
There are numerous possible causes for this failure :
- The scan may have caused a service to freeze or stop running.
- An administrator may have stopped a particular service during the scanning process.
This might be an availability problem related to the following reasons :
- A network outage has been experienced during the scan, and the remote network cannot be reached from the Vulnerability Scanner any more.
- This Vulnerability Scanner has been blacklisted by the system administrator or by automatic intrusion detection/ prevention systems which have detected the vulnerability assessment.
- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.
In any case, the audit of the remote host might be incomplete and may need to be done again

Solution

- increase checks_read_timeout and/or reduce max_checks
- disable your IPS during the Nessus scan

Risk Factor

None

Hosts

192.168.1.200 (tcp/0)

```
Port 8887 was detected as being open but is now closed
Port 8060 was detected as being open but is now closed
Port 8080 was detected as being open but is now closed
```

10940 (1) - Windows Terminal Services Enabled

Synopsis

The remote Windows host has Terminal Services enabled.

Description

Terminal Services allows a Windows user to remotely obtain a graphical login (and therefore act as a local user on the remote host).

If an attacker gains a valid login and password, he may be able to use this service to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.

Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.

Solution

Disable Terminal Services if you do not use it, and do not allow this service to run across the Internet.

Risk Factor

None

Hosts

192.168.1.16 (tcp/3389)

11026 (1) - Wireless Access Point Detection

Synopsis

The remote host is a wireless access point.

Description

Nessus has determined that the remote host is a wireless access point (AP).
Ensure that proper physical and logical controls are in place for its use. A misconfigured access point may allow an attacker to gain access to an internal network without being physically present on the premises. If the access point is using an 'off-the-shelf'
configuration (such as 40 or 104 bit WEP encryption), the data being passed through the access point may be vulnerable to hijacking or sniffing.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.80 (tcp/0)

```
Nessus has classified this device as a wireless-access-point based on
its OS fingerprint.
```

11153 (1) - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.16 (tcp/2869)

```
A web server seems to be running on this port.
```

11819 (1) - TFTP Daemon Detection

Synopsis

A TFTP server is listening on the remote port.

Description

The remote host is running a TFTP (Trivial File Transfer Protocol) daemon. TFTP is often used by routers and diskless hosts to retrieve their configuration. It is also used by worms to propagate.

Solution

Disable this service if you do not use it.

Risk Factor

None

Hosts

192.168.1.80 (udp/69)

11933 (1) - Do not scan printers

Synopsis

The remote host appears to be a fragile device and will not be scanned.

Description

The remote host appears to be a network printer, multi-function device, or other fragile device. Such devices often react very poorly when scanned. To avoid problems, Nessus has marked the remote host as 'Dead' and will not scan it.

Solution

If you are not concerned about such behavior, enable the 'Scan Network Printers' setting under the 'Do not scan fragile devices' advanced settings block and re-run the scan.

Risk Factor

None

Hosts

192.168.1.245 (tcp/0)

```
HP printer-related web server on port 80.
```

12634 (1) - Authenticated Check: OS Name and Installed Package Enumeration

Synopsis

This plugin gathers information about the remote host via an authenticated session.

Description

This plugin logs into the remote host using SSH, RSH, RLOGIN, Telnet or local commands and extracts the list of installed packages.

If using SSH, the scan should be configured with a valid SSH public key and possibly an SSH passphrase (if the SSH public key is protected by a passphrase).

Solution

n/a

Risk Factor

None

Hosts

192.168.1.248 (tcp/0)

```
Nessus can run commands on localhost to check if patches are
applied.

The output of "uname -a" is :
Linux NESSUSSERVER 2.6.39.4 #1 SMP Thu Aug 18 13:38:02 NZST 2011 i686 GNU/Linux

The remote Debian system is :
squeeze/sid

This is a Ubuntu system

Local security checks have been enabled for this host.
```

17651 (1) - Microsoft Windows SMB : Obtains the Password Policy

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.30 (tcp/445)

```
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0
```

17975 (1) - Service Detection (GET request)

Synopsis

The remote service could be identified.

Description

It was possible 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

Hosts

192.168.1.213 (tcp/8080)

```
The remote service appears to be a control channel for a Roku
Streaming Player.  Not only does the the banner reveal the Device ID
associated with the player as well as its Ethernet and Wifi MACs
addresses, but it's also possible to control the device by sending
commands such as 'press up' and 'press home' to this service.
```

18261 (1) - 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

This script extracts the banner of the Apache web server and attempts to 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

Hosts

192.168.1.248 (tcp/0)

```
The linux distribution detected was :
 - Ubuntu 10.04 (lucid)
```

20108 (1) - Web Server / Application favicon.ico Vendor Fingerprinting

Synopsis

The remote web server contains a graphic image that is prone to information disclosure.

Description

The 'favicon.ico' file found on the remote web server belongs to a popular webserver. This may be used to fingerprint the web server.

Solution

Remove the 'favicon.ico' file or create a custom one for your site.

Risk Factor

None

References

XREF	OSVDB:39272

Hosts

192.168.1.231 (tcp/8834)

```
The MD5 fingerprint for 'favicon.ico' suggests the web server is Nessus 4.x Web Client.
```

20217 (1) - iTunes Music Sharing Enabled

Synopsis

The remote host contains an application that may not match your corporate security policy.

Description

The version of iTunes on the remote host is configured to stream music between hosts.
Such song sharing may not be in accordance with your security policy.

Solution

Disable song sharing if desired or limit access to this port.

Risk Factor

None

Hosts

192.168.1.231 (tcp/3689)

20301 (1) - VMware ESX/GSX Server detection

Synopsis

The remote host appears to be running VMware Server, ESX Server, or GSX Server.

Description

According to its banner, the remote host appears to be running a VMware server authentication daemon, which likely indicates the remote host is running VMware Server, ESX Server, or GSX Server.

See Also

http://www.vmware.com/

Solution

n/a

Risk Factor

None

Hosts

192.168.1.16 (tcp/912)

20813 (1) - TiVo Detection

Synopsis

The remote host is a personal video recorder (PVR).

Description

The remote host is a TiVo, a personal video recorder.

Solution

Make sure that use of such devices is in line with your organization's security policy.

Risk Factor

None

Hosts

192.168.1.81 (tcp/0)

```
The remote TiVO is running TiVO software version 20.2-01-2:746
```

22869 (1) - Software Enumeration (SSH)

Synopsis

It is possible to enumerate installed software on the remote host, via SSH.

Description

This plugin lists the software installed on the remote host by calling the appropriate command (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

Hosts

192.168.1.248 (tcp/0)

```
Here is the list of packages installed on the remote Linux system :

  +++-============================================-============================================-
=========================================================================================================
  Desired=Unknown/Install/Remove/Purge/Hold
  ii  0trace                                       1.0-bt4
 0trace is a traceroute tool that can be run within an existing, open TCP connection - therefore
 bypassin
  ii  3proxy                                       0.6.1-bt2
 3APA3A 3proxy tiny proxy server
  ii  ace                                          1.10-bt2
     ACE (Automated Corporate Enumerator) is a simple yet powerful VoIP Corporate Directory
 enumeration tool
  ii  adduser                                      3.112ubuntu1
 add and remove users and groups
  ii  admsnmp                                       [...]
```

25240 (1) - Samba Server Detection

Synopsis

An SMB server is running on the remote host.

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

See Also

http://www.samba.org/

Solution

n/a

Risk Factor

None

Hosts

192.168.1.30 (tcp/445)

26917 (1) - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.
If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access'
service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.16 (tcp/445)

```
Could not connect to the registry because:
Could not connect to \winreg
```

35712 (1) - Web Server UPnP Detection

Synopsis

The remote web server provides UPnP information.

Description

It was possible to extract some information about the UPnP-enabled device by querying this web server.
Services may also be reachable through SOAP requests.

See Also

http://en.wikipedia.org/wiki/Universal_Plug_and_Play

Solution

Filter incoming traffic to this port if desired.

Risk Factor

None

Hosts

192.168.1.213 (tcp/8060)

```
Here is a summary of http://192.168.1.213:8060/ :

deviceType:urn:schemas-upnp-org:device:MediaRenderer:1
friendlyName:Roku Streaming Player
manufacturer:Roku
manufacturerURL:http://www.roku.com/
modelDescription:Roku Streaming Player Network Media
modelName:Roku Streaming Player N1101
modelNumber:N1101
modelURL:http://www.roku.com/
serialNumber:D0C9DP009064
```

39521 (1) - 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

http://www.nessus.org/u?d636c8c7

Solution

N/A

Risk Factor

None

Hosts

192.168.1.248 (tcp/80)

42410 (1) - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

Synopsis

It is possible to obtain the network name of the remote host.

Description

The remote host listens on tcp port 445 and replies to SMB requests.
By sending an NTLMSSP authentication request it is possible to obtain the name of the remote system and the name of its domain.

Solution

n/a

Risk Factor

None

Hosts

192.168.1.16 (tcp/445)

```
The following 2 NetBIOS names have been gathered :

 O-REN            = Computer name
 O-REN            = Workgroup / Domain name
```

42825 (1) - Apple TV Detection

Synopsis

The remote host is a digital media receiver.

Description

The remote host is an Apple TV, a digital media receiver.

See Also

http://www.apple.com/appletv/

Solution

Make sure that use of such devices is in line with your organization's acceptable use and security policies.

Risk Factor

None

Hosts

192.168.1.211 (tcp/0)

44318 (1) - HNAP Detection

Synopsis

The remote device has HNAP enabled.

Description

The remote service supports the Home Network Administration Protocol (HNAP), a SOAP-based protocol that provides a common interface for administrative control of networked devices.

See Also

http://www.hnap.org/

http://www.nessus.org/u?1b0ee657

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Hosts

192.168.1.80 (tcp/80)

44391 (1) - Linksys Router Detection

Synopsis

The remote device is a Linksys router.

Description

The remote device is a Linksys router. These devices route packets and may provide port forwarding, DMZ configuration and other networking services.

See Also

http://www.linksysbycisco.com/

Solution

Ensure that use of this device agrees with your organization's acceptable use and security policies.

Risk Factor

None

Hosts

192.168.1.80 (tcp/80)

```
Model             : WET610N
Description       : Dual-Band Wireless-N Gaming and Video Adapter
Firmware        : 1.0.03 build 351
```

46212 (1) - PVS Proxy Detection

Synopsis

A proxy service is listening on this port.

Description

The remote service appears to be a Tenable Network Security proxy for either the Passive Vulnerability Scanner (PVS) or the Security Center 3 proxy.

PVS monitors network traffic in real-time, detecting server and client vulnerabilities, and a PVS proxy is used by Tenable's SecurityCenter 4 to transfer report data between a PVS sensor and a SecurityCenter console.

The Security Center 3 proxy is in place for legacy communication requirements.

See Also

http://www.nessus.org/products/pvs/

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Hosts

192.168.1.13 (tcp/1243)

50845 (1) - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its behavior, it seems that the remote service is using the OpenSSL library to encrypt traffic.
Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

http://www.openssl.org

Solution

n/a

Risk Factor

None

Hosts

192.168.1.81 (tcp/443)

53513 (1) - Link-Local Multicast Name Resolution (LLMNR) Detection

Synopsis

The remote device supports LLMNR.

Description

The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions.

See Also

http://www.nessus.org/u?85beb421

http://technet.microsoft.com/en-us/library/bb878128.aspx

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

Risk Factor

None

Hosts

192.168.1.16 (udp/5355)

```
According to LLMNR, the name of the remote host is 'O-Ren'.
```

55472 (1) - Device Hostname

Synopsis

It is 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

Hosts

192.168.1.248 (tcp/0)

```
Hostname : NESSUSSERVER
```

56693 (1) - Dropbox Software Detection (uncredentialed check)

Synopsis

There is a file synchronization application on the remote host.

Description

Dropbox is installed on the remote host. Dropbox is an application for storing and synchronizing files between computers, possibly outside the organization.

See Also

https://www.dropbox.com/

Solution

Ensure that use of this software agrees with your organization's acceptable use and security policies.

Risk Factor

None

Hosts

192.168.1.231 (tcp/17500)

```
The remote DropBox server broadcasts the following data :
{"host_int": 77339174, "version": [1, 8], "displayname": "77339174", "port": 17500, "namespaces":
 [69385827, 82845516, 61346060, 54162449, 69420146, 6768627, 58215509, 58372182]}
```