

Audit Report

Metasploitable

Audited on May 2, 2015

Reported on May 3, 2015

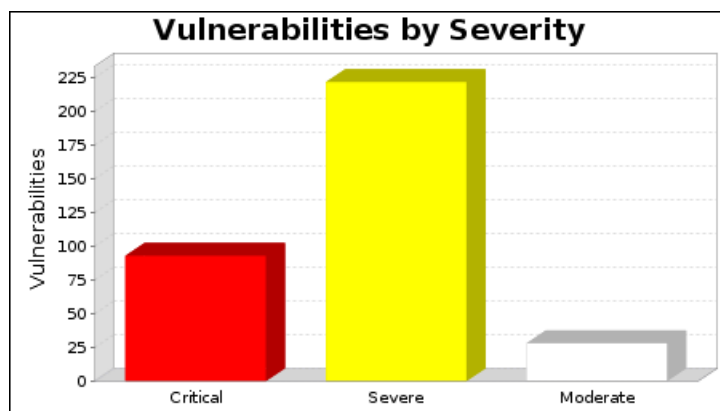
1. Executive Summary

This report represents a security audit performed by Nexpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

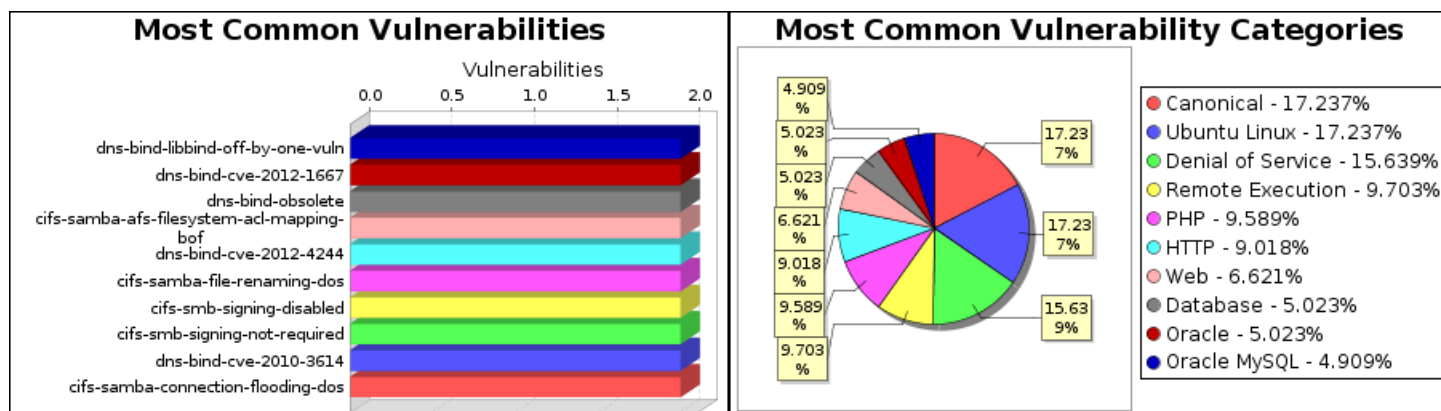
Site Name	Start Time	End Time	Total Time	Status
Metasploitable	May 02, 2015 23:35, ADT	May 03, 2015 00:11, ADT	35 minutes	Success

There is not enough historical data to display risk trend.

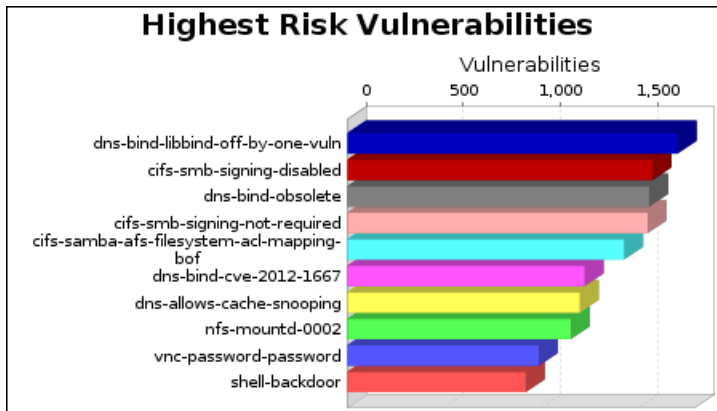
The audit was performed on one system which was found to be active and was scanned.



There were 343 vulnerabilities found during this scan. Of these, 93 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 222 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 28 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.



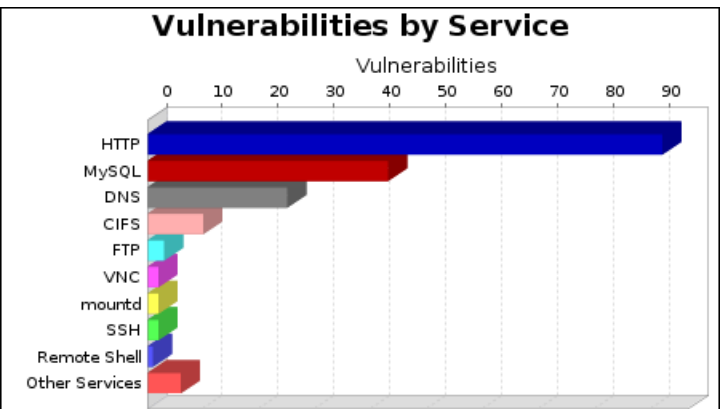
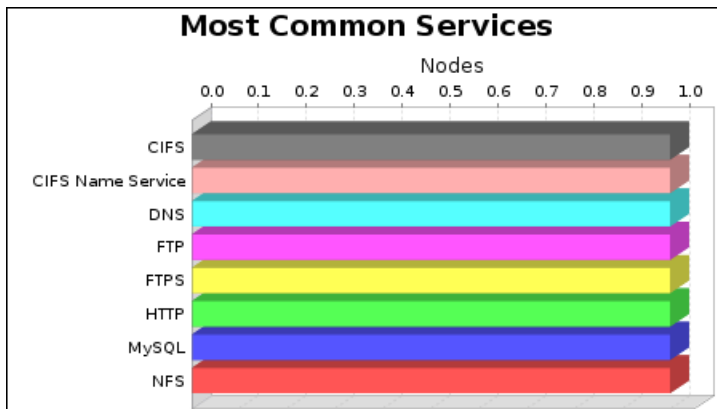
There were 2 occurrences of the dns-bind-libbind-off-by-one-vuln, dns-bind-cve-2012-1667, dns-bind-obsolete, cifs-samba-afs-filesystem-acl-mapping-bof, dns-bind-cve-2012-4244, cifs-samba-file-renaming-dos, cifs-smb-signing-disabled, cifs-smb-signing-not-required, dns-bind-cve-2010-3614 and cifs-samba-connection-flooding-dos vulnerabilities, making them the most common vulnerabilities. There were 151 vulnerabilities in the Canonical and Ubuntu Linux categories, making them the most common vulnerability categories.



The dns-bind-libbind-off-by-one-vuln vulnerability poses the highest risk to the organization with a risk score of 1,700. Risk scores are based on the types and numbers of vulnerabilities on affected assets.

One operating system was identified during this scan.

There were 25 services found to be running during this scan.



The CIFS, CIFS Name Service, DNS, FTP, FTPS, HTTP, MySQL and NFS services were found on 1 systems, making them the most common services. The HTTP service was found to have the most vulnerabilities during this scan with 92 vulnerabilities.

2. Discovered Systems

Node	Operating System	Risk	Aliases
192.168.0.102	Ubuntu Linux 8.04	150,684	•METASPLOITABLE

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

3.1.1. Tomcat Application Manager Tomcat Tomcat Password Vulnerability (apache-tomcat-default-password)

Description:

HP Operations Manager 8.10 on Windows contains a "hidden account" in the XML file that specifies Tomcat users, which allows remote attackers to conduct unrestricted file upload attacks, and thereby execute arbitrary code, by using the `org.apache.catalina.manager.HTMLManagerServlet` class to make requests to `manager/html/upload`.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:8180	<p>Running HTTP serviceProduct Tomcat exists -- Apache TomcatBased on the following 2 results:HTTP GET request to http://192.168.0.102:8180/manager/html HTTP response code was an expected 401</p> <p>HTTP GET request to http://192.168.0.102:8180/manager/html HTTP response code was an expected 200</p> <p>82: 84: 85: 82: ...="0" alt="The Tomcat Servlet/JSP Container"</p>

References:

Source	Reference
BID	38084
CVE	CVE-2009-3843
CVE	CVE-2010-0557
OSVDB	60317
OSVDB	62118
XF	54361

Vulnerability Solution:

The Tomcat service has an administrator account set to a default configuration. This can be easily changed in conf/tomcat-users.xml

3.1.2. ISC BIND: inet_network() off-by-one buffer overflow (CVE-2008-0122) (dns-bind-libbind-off-by-one-vuln)

Description:

Off-by-one error in the inet_network function in libbind in ISC BIND 9.4.2 and earlier, as used in libc in FreeBSD 6.2 through 7.0-PRERELEASE, allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted input that triggers memory corruption.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2

References:

Source	Reference
BID	27283
CERT-VN	203611
CVE	CVE-2008-0122
OVAL	OVAL10190
REDHAT	RHSA-2008:0300
URL	https://kb.isc.org/article/AA-00923/0
URL	https://kb.isc.org/article/AA-00923/187/CVE-2008-0122%3A-Buffer-overflow-in-inet_network.html
XF	39670

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the [ISC website](#).

3.1.3. CVE-2014-6271 bash: specially-crafted environment variables can be used to inject shell commands (gnu-bash-cve-2014-6271)

Description:

GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Execute command: <code>env x='() { :; }; echo CVE-2014-6271' bash -c exit</code> Standard output matched: 1: CVE-2014-6271

References:

Source	Reference
CVE	CVE-2014-6271
URL	https://securityblog.redhat.com/2014/09/24/bash-specially-crafted-environment-variables-code-injection-attack/

Vulnerability Solution:

Use your operating system's package manager to upgrade GNU bash to the latest version.

3.1.4. CVE-2014-6278 bash: code execution via specially crafted environment variables (gnu-bash-cve-2014-6278)*Description:*

GNU Bash through 4.3 bash43-026 does not properly parse function definitions in the values of environment variables, which allows remote attackers to execute arbitrary commands via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271, CVE-2014-7169, and CVE-2014-6277.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Execute command: <code>x='() { echo Vulnerable; }' bash -c x</code> Standard output matched: 1: Vulnerable

References:

Source	Reference
CVE	CVE-2014-6278

Vulnerability Solution:

Use your operating system's package manager to upgrade GNU bash to the latest version.

3.1.5. CVE-2014-7169 bash: specially-crafted environment variables can be used to inject shell commands (gnu-bash-cve-2014-7169)

Description:

GNU Bash through 4.3 bash43-025 processes trailing strings after certain malformed function definitions in the values of environment variables, which allows remote attackers to write to files or possibly have unknown other impact via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	<p>Execute command: env x=() { (a)=>' bash -c "shellsh0ck echo CVE-2014-7169"; cat shellsh0ck; rm shellsh0ck</p> <p>Standard output matched:</p> <p>4: bash: x: line 1: syntax error near unexpected token `='</p> <p>5: bash: x: line 1: ``</p> <p>6: bash: error importing function definition for `x'</p> <p>4: CVE-2014-7169</p>

References:

Source	Reference
CVE	CVE-2014-7169

Vulnerability Solution:

Use your operating system's package manager to upgrade GNU bash to the latest version.

3.1.6. CVE-2014-7186 bash: parser can allow out-of-bounds memory access while handling redir_stack (gnu-bash-cve-2014-7186)

Description:

The redirection implementation in `parse.y` in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified other impact via crafted use of here documents, aka the "redir_stack" issue.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	<p>Execute command: bash -c 'true <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF' echo CVE-2014-7186</p> <p>Standard output matched:</p> <p>3: bash: [4990: 3] tcsetattr: Invalid argument</p> <p>4: Segmentation fault</p>

Affected Nodes:	Additional Information:
	3: CVE-2014-7186

References:

Source	Reference
CVE	CVE-2014-7186

Vulnerability Solution:

Use your operating system's package manager to upgrade GNU bash to the latest version.

3.1.7. PHP Multiple Vulnerabilities Fixed in version 5.2.12 ([http-php-multiple-vulns-5-2-12](#))*Description:*

PHP before 5.2.12 does not properly handle session data, which has unspecified impact and attack vectors related to (1) interrupt corruption of the SESSION superglobal array and (2) the session.save_path directive.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
BID	37389
BID	37390
CVE	CVE-2009-3557
CVE	CVE-2009-3558
CVE	CVE-2009-4017
CVE	CVE-2009-4142
CVE	CVE-2009-4143
DEBIAN	DSA-1940
DEBIAN	DSA-2001
OVAL	OVAL10005
OVAL	OVAL10483
OVAL	OVAL6667
OVAL	OVAL7085

Source	Reference
OVAL	OVAL7396
OVAL	OVAL7439
URL	http://www.php.net/ChangeLog-5.php#5.2.12
URL	http://www.php.net/releases/5_2_12.php
XF	54455

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.12.tar.gz>

3.1.8. PHP Multiple Vulnerabilities Fixed in version 5.2.8 (http-php-multiple-vulns-5-2-8)*Description:*

Heap-based buffer overflow in ext/mbstring/libmbfl/filters/mbfilter_htmlent.c in the mbstring extension in PHP 4.3.0 through 5.2.6 allows context-dependent attackers to execute arbitrary code via a crafted string containing an HTML entity, which is not properly handled during Unicode conversion, related to the (1) mb_convert_encoding, (2) mb_check_encoding, (3) mb_convert_variables, and (4) mb_parse_str functions.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2008-10-09
APPLE	APPLE-SA-2009-05-12
BID	30087
BID	31681
BID	32383
BID	32625
BID	32673
BID	32688
BID	32948
CERT	TA09-133A
CVE	CVE-2008-2371
CVE	CVE-2008-5557

Source	Reference
CVE	CVE-2008-5624
CVE	CVE-2008-5625
CVE	CVE-2008-5658
CVE	CVE-2008-5844
DEBIAN	DSA-1602
DEBIAN	DSA-1789
OSVDB	50480
OSVDB	50483
OSVDB	52205
OSVDB	52207
OVAL	OVAL10286
REDHAT	RHSA-2009:0350
URL	http://bugs.php.net/bug.php?id=42718
URL	http://bugs.php.net/bug.php?id=45722
URL	http://www.php.net/ChangeLog-5.php#5.2.8
XF	47079
XF	47314
XF	47318
XF	47525

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.8.tar.gz>

3.1.9. MySQL Obsolete Version (mysql-obsolete-version)*Description:*

An obsolete version of the MySQL database server is running. Oracle classifies the support lifecycle for its MySQL product versions into Premier Support, Extended Support and Sustain Support. Extended and Premier support for 5.1 ended on December 31st, 2013. Note: When the support period ends for a MySQL product, no further patches will be provided even for serious security problems.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
URL	http://www.mysql.com/company/legal/lifecycle/
URL	http://www.mysql.com/support/eol-notice.html

Vulnerability Solution:

Download and apply the upgrade from: <http://dev.mysql.com/downloads/mysql>

3.1.10. PHP Vulnerability: CVE-2011-3268 (php-cve-2011-3268)*Description:*

Buffer overflow in the crypt function in PHP before 5.3.7 allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2012-02-01-1
BID	49241
CVE	CVE-2011-3268
OSVDB	74738
XF	69427

Vulnerability Solution:

Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.11. PHP Vulnerability: CVE-2012-2688 (php-cve-2012-2688)*Description:*

Unspecified vulnerability in the _php_stream_scandir function in the stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an "overflow."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
CVE	CVE-2012-2688
DEBIAN	DSA-2527
REDHAT	RHSA-2013:1307

Vulnerability Solution:

- Upgrade to PHP version 5.3.15
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.4.5
Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.12. Shell Backdoor Service (shell-backdoor)*Description:*

A non-standard service was found that provides a means to establish local shell access on the host over the network.

Note: The presence of a "backdoor" is a serious security concern. It indicates a high probability that this asset has been compromised and is at risk of being leveraged by malicious users.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:1524	Running Shell Backdoor service

References:

None

Vulnerability Solution:

Determine the mechanism used to create the backdoor and safely disable or remove it.

3.1.13. Obsolete Version of Ubuntu (ubuntu-obsolete-version)*Description:*

This release has passed its End of Life. There may be unpatched security vulnerabilities. Please check with <https://wiki.ubuntu.com/Releases> for supported versions.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04

References:

None

Vulnerability Solution:

Upgrade to a supported version of Ubuntu Linux

3.1.14. USN-1403-1: FreeType vulnerabilities (ubuntu-usn-1403-1)*Description:*

FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via crafted property data in a BDF font.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libfreetype6 2.3.5-1ubuntu4.8.04.2

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-1
CVE	CVE-2012-1126
CVE	CVE-2012-1127
CVE	CVE-2012-1128
CVE	CVE-2012-1129
CVE	CVE-2012-1130
CVE	CVE-2012-1131
CVE	CVE-2012-1132
CVE	CVE-2012-1133
CVE	CVE-2012-1134
CVE	CVE-2012-1135

Source	Reference
CVE	CVE-2012-1136
CVE	CVE-2012-1137
CVE	CVE-2012-1138
CVE	CVE-2012-1139
CVE	CVE-2012-1140
CVE	CVE-2012-1141
CVE	CVE-2012-1142
CVE	CVE-2012-1143
CVE	CVE-2012-1144
DEBIAN	DSA-2428
REDHAT	RHSA-2012:0467
USN	USN-1403-1

Vulnerability Solution:

- libfreetype6 on Ubuntu Linux 10.04

Upgrade libfreetype6 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

- libfreetype6 on Ubuntu Linux 10.10

Upgrade libfreetype6 for Ubuntu 10.10

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

- libfreetype6 on Ubuntu Linux 11.04

Upgrade libfreetype6 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

- libfreetype6 on Ubuntu Linux 11.10

Upgrade libfreetype6 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

- libfreetype6 on Ubuntu Linux 8.04

Upgrade libfreetype6 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

3.1.15. USN-1423-1: Samba vulnerability (ubuntu-usn-1423-1)

Description:

The RPC code generator in Samba 3.x before 3.4.16, 3.5.x before 3.5.14, and 3.6.x before 3.6.4 does not implement validation of an array length in a manner consistent with validation of array memory allocation, which allows remote attackers to execute arbitrary code via a crafted RPC call.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu samba 3.0.20-0.1ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2012-05-09-1
CVE	CVE-2012-1182
USN	USN-1423-1

Vulnerability Solution:

- samba on Ubuntu Linux 10.04
Upgrade samba for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade samba to the latest version
- samba on Ubuntu Linux 11.04
Upgrade samba for Ubuntu 11.04
Use `apt-get upgrade` to upgrade samba to the latest version
- samba on Ubuntu Linux 11.10
Upgrade samba for Ubuntu 11.10
Use `apt-get upgrade` to upgrade samba to the latest version
- samba on Ubuntu Linux 8.04
Upgrade samba for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade samba to the latest version

3.1.16. USN-613-1: GnuTLS vulnerabilities (ubuntu-usn-613-1)*Description:*

The `_gnutls_server_name_rcv_params` function in `lib/ext_server_name.c` in `libgnutls` in `gnutls-serv` in GnuTLS before 2.2.4 does not properly calculate the number of Server Names in a TLS 1.0 Client Hello message during extension handling, which allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a zero value for the length of Server Names, which leads to a buffer overflow in session resumption data in the `pack_security_parameters` function, aka GNUTLS-SA-2008-1-1.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libgnutls13 2.0.4-1ubuntu2

References:

Source	Reference
BID	29292
CERT-VN	111034
CERT-VN	252626
CERT-VN	659209
CVE	CVE-2008-1948
CVE	CVE-2008-1949
CVE	CVE-2008-1950
DEBIAN	DSA-1581
OVAL	OVAL10935
OVAL	OVAL11393
OVAL	OVAL9519
REDHAT	RHSA-2008:0489
REDHAT	RHSA-2008:0492
SUSE	SUSE-SA:2008:046
USN	USN-613-1
XF	42530
XF	42532
XF	42533

Vulnerability Solution:

- libgnutls13 on Ubuntu Linux 7.04
Upgrade libgnutls13 for Ubuntu 7.04
Use `apt-get upgrade` to upgrade libgnutls13 to the latest version
- libgnutls13 on Ubuntu Linux 7.10
Upgrade libgnutls13 for Ubuntu 7.10
Use `apt-get upgrade` to upgrade libgnutls13 to the latest version
- libgnutls13 on Ubuntu Linux 8.04
Upgrade libgnutls13 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libgnutls13 to the latest version

3.1.17. USN-644-1: libxml2 vulnerabilities (ubuntu-usn-644-1)*Description:*

Heap-based buffer overflow in the xmlParseAttValueComplex function in parser.c in libxml2 before 2.7.0 allows context-dependent attackers to cause a denial of service (crash) or execute arbitrary code via a long XML entity name.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libxml2 2.6.31.dfsg-2ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2009-05-12
APPLE	APPLE-SA-2009-06-08-1
APPLE	APPLE-SA-2009-06-17-1
BID	30783
BID	31126
CERT	TA09-133A
CVE	CVE-2008-3281
CVE	CVE-2008-3529
DEBIAN	DSA-1631
DEBIAN	DSA-1654
OVAL	OVAL11760
OVAL	OVAL6103
OVAL	OVAL6496
OVAL	OVAL9812
REDHAT	RHSA-2008:0836
REDHAT	RHSA-2008:0884
REDHAT	RHSA-2008:0886
USN	USN-644-1
XF	45085

Vulnerability Solution:

•libxml2 on Ubuntu Linux 7.04

Upgrade libxml2 for Ubuntu 7.04

Use `apt-get upgrade` to upgrade libxml2 to the latest version

•libxml2 on Ubuntu Linux 7.10

Upgrade libxml2 for Ubuntu 7.10

Use `apt-get upgrade` to upgrade libxml2 to the latest version

- libxml2 on Ubuntu Linux 8.04

Upgrade libxml2 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version

3.1.18. USN-673-1: libxml2 vulnerabilities (ubuntu-usn-673-1)

Description:

Integer overflow in the xmlSAX2Characters function in libxml2 2.7.2 allows context-dependent attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a large XML document.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libxml2 2.6.31.dfsg-2ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2009-06-08-1
APPLE	APPLE-SA-2009-06-17-1
BID	32326
BID	32331
CVE	CVE-2008-4225
CVE	CVE-2008-4226
DEBIAN	DSA-1666
OSVDB	49992
OSVDB	49993
OVAL	OVAL10025
OVAL	OVAL6219
OVAL	OVAL6234
OVAL	OVAL6360
OVAL	OVAL6415
OVAL	OVAL9888
REDHAT	RHSA-2008:0988
USN	USN-673-1

Vulnerability Solution:

- libxml2 on Ubuntu Linux 7.10

Upgrade libxml2 for Ubuntu 7.10

Use `apt-get upgrade` to upgrade libxml2 to the latest version

- libxml2 on Ubuntu Linux 8.04

Upgrade libxml2 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version

- libxml2 on Ubuntu Linux 8.10

Upgrade libxml2 for Ubuntu 8.10

Use `apt-get upgrade` to upgrade libxml2 to the latest version

3.1.19. USN-762-1: APT vulnerabilities (ubuntu-usn-762-1)

Description:

apt 0.7.20 does not check when the date command returns an "invalid date" error, which can prevent apt from loading security updates in time zones for which DST occurs at midnight.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu apt 0.7.9ubuntu17

References:

Source	Reference
CVE	CVE-2009-1300
DEBIAN	DSA-1779
USN	USN-762-1

Vulnerability Solution:

- apt on Ubuntu Linux 8.04

Upgrade apt for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade apt to the latest version

- apt on Ubuntu Linux 8.10

Upgrade apt for Ubuntu 8.10

Use `apt-get upgrade` to upgrade apt to the latest version

3.1.20. USN-803-1: dhcp vulnerability (ubuntu-usn-803-1)

Description:

Stack-based buffer overflow in the script_write_params method in client/dhclient.c in ISC DHCP dhclient 4.1 before 4.1.0p1, 4.0 before 4.0.1p1, 3.1 before 3.1.2p1, 3.0, and 2.0 allows remote DHCP servers to execute arbitrary code via a crafted subnet-mask option.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu dhcp3-client 3.0.6.dfsg-1ubuntu9

References:

Source	Reference
BID	35668
CERT-VN	410676
CVE	CVE-2009-0692
DEBIAN	DSA-1833
NETBSD	NetBSD-SA2009-010
OSVDB	55819
OVAL	OVAL10758
OVAL	OVAL5941
REDHAT	RHSA-2009:1136
REDHAT	RHSA-2009:1154
SUSE	SUSE-SA:2009:037
USN	USN-803-1

Vulnerability Solution:

- dhcp3-client on Ubuntu Linux 8.04
Upgrade dhcp3-client for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade dhcp3-client to the latest version
- dhcp3-client on Ubuntu Linux 8.10
Upgrade dhcp3-client for Ubuntu 8.10
Use `apt-get upgrade` to upgrade dhcp3-client to the latest version
- dhcp3-client on Ubuntu Linux 9.04
Upgrade dhcp3-client for Ubuntu 9.04
Use `apt-get upgrade` to upgrade dhcp3-client to the latest version
- dhcp3-client-udeb on Ubuntu Linux 8.04
Upgrade dhcp3-client-udeb for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade dhcp3-client-udeb to the latest version

- dhcp3-client-udeb on Ubuntu Linux 8.10

Upgrade dhcp3-client-udeb for Ubuntu 8.10

Use `apt-get upgrade` to upgrade dhcp3-client-udeb to the latest version

- dhcp3-client-udeb on Ubuntu Linux 9.04

Upgrade dhcp3-client-udeb for Ubuntu 9.04

Use `apt-get upgrade` to upgrade dhcp3-client-udeb to the latest version

3.1.21. USN-813-1: apr vulnerability (ubuntu-usn-813-1)

Description:

Multiple integer overflows in the Apache Portable Runtime (APR) library and the Apache Portable Utility library (aka APR-util) 0.9.x and 1.3.x allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors that trigger crafted calls to the (1) allocator_alloc or (2) apr_palloc function in memory/unix/apr_pools.c in APR; or crafted calls to the (3) apr_rmm_malloc, (4) apr_rmm_calloc, or (5) apr_rmm_realloc function in misc/apr_rmm.c in APR-util; leading to buffer overflows. NOTE: some of these details are obtained from third party information.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libapr1 1.2.11-1

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
BID	35949
CVE	CVE-2009-2412
OSVDB	56765
OSVDB	56766
OVAL	OVAL8394
OVAL	OVAL9958
SUSE	SUSE-SA:2009:050
USN	USN-813-1

Vulnerability Solution:

- libapr1 on Ubuntu Linux 8.04

Upgrade libapr1 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libapr1 to the latest version

- libapr1 on Ubuntu Linux 8.10

Upgrade libapr1 for Ubuntu 8.10

Use `apt-get upgrade` to upgrade libapr1 to the latest version

- libapr1 on Ubuntu Linux 9.04

Upgrade libapr1 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade libapr1 to the latest version

3.1.22. USN-813-3: apr-util vulnerability (ubuntu-usn-813-3)

Description:

Multiple integer overflows in the Apache Portable Runtime (APR) library and the Apache Portable Utility library (aka APR-util) 0.9.x and 1.3.x allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors that trigger crafted calls to the (1) allocator_alloc or (2) apr_palloc function in memory/unix/apr_pools.c in APR; or crafted calls to the (3) apr_rmm_malloc, (4) apr_rmm_calloc, or (5) apr_rmm_realloc function in misc/apr_rmm.c in APR-util; leading to buffer overflows.

NOTE: some of these details are obtained from third party information.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libaprutil1 1.2.12+dfsg-3

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
BID	35949
CVE	CVE-2009-2412
OSVDB	56765
OSVDB	56766
OVAL	OVAL8394
OVAL	OVAL9958
SUSE	SUSE-SA:2009:050
USN	USN-813-3

Vulnerability Solution:

- libaprutil1 on Ubuntu Linux 8.04

Upgrade libaprutil1 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libaprutil1 to the latest version

- libaprutil1 on Ubuntu Linux 8.10

Upgrade libaprutil1 for Ubuntu 8.10

Use `apt-get upgrade` to upgrade libaprutil1 to the latest version

- libaprutil1 on Ubuntu Linux 9.04

Upgrade libaprutil1 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade libaprutil1 to the latest version

3.1.23. USN-815-1: libxml2 vulnerabilities (ubuntu-usn-815-1)

Description:

Heap-based buffer overflow in the xmlParseAttValueComplex function in parser.c in libxml2 before 2.7.0 allows context-dependent attackers to cause a denial of service (crash) or execute arbitrary code via a long XML entity name.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libxml2 2.6.31.dfsg-2ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2009-05-12
APPLE	APPLE-SA-2009-06-08-1
APPLE	APPLE-SA-2009-06-17-1
APPLE	APPLE-SA-2009-11-09-1
APPLE	APPLE-SA-2009-11-11-1
APPLE	APPLE-SA-2010-06-21-1
BID	31126
BID	36010
CERT	TA09-133A
CVE	CVE-2008-3529
CVE	CVE-2009-2414
CVE	CVE-2009-2416
DEBIAN	DSA-1654
DEBIAN	DSA-1859
DISA_SEVERITY	Category I

Source	Reference
DISA_VMSKEY	V0019911
IAVM	2009-T-0049
OVAL	OVAL10129
OVAL	OVAL11760
OVAL	OVAL6103
OVAL	OVAL7783
OVAL	OVAL8639
OVAL	OVAL9262
REDHAT	RHSA-2008:0884
REDHAT	RHSA-2008:0886
USN	USN-815-1
XF	45085

Vulnerability Solution:

- libxml2 on Ubuntu Linux 8.04

Upgrade libxml2 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version

- libxml2 on Ubuntu Linux 8.10

Upgrade libxml2 for Ubuntu 8.10

Use `apt-get upgrade` to upgrade libxml2 to the latest version

- libxml2 on Ubuntu Linux 9.04

Upgrade libxml2 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade libxml2 to the latest version

3.1.24. VNC password is "password" (vnc-password-password)

Description:

The VNC server is using the password "password". This would allow anyone to log into the machine via VNC and take complete control.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:5900	Running VNC serviceSuccessfully authenticated to the VNC service with credentials: uid[] pw[password] realm[]

References:

None

Vulnerability Solution:

Change the password to a stronger, unpredictable one.

3.1.25. ISC BIND: Handling of zero length rdata can cause named to terminate unexpectedly (CVE-2012-1667) (dns-bind-cve-2012-1667)

Description:

ISC BIND 9.x before 9.7.6-P1, 9.8.x before 9.8.3-P1, 9.9.x before 9.9.1-P1, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P1 does not properly handle resource records with a zero-length RDATA section, which allows remote DNS servers to cause a denial of service (daemon crash or data corruption) or obtain sensitive information from process memory via a crafted record.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
CVE	CVE-2012-1667
DISA_SEVERITY	Category I
DISA_VMSKEY	V0035032
IAVM	2012-A-0189
REDHAT	RHSA-2012:1110
URL	https://kb.isc.org/article/AA-00698/0
URL	https://kb.isc.org/article/AA-00698/74/CVE-2012-1667%3A-Handling-of-zero-length-rdata-can-cause-named-to-terminate-unexpectedly.html

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the [ISC website](#).

3.1.26. Obsolete ISC BIND installation (dns-bind-obsolete)

Description:

ISC BIND versions before 9.9 are considered obsolete. ISC will not fix security bugs in these versions (even critical ones).

It is strongly recommended that you upgrade your BIND installation to a supported version.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2

References:

Source	Reference
URL	https://kb.isc.org/article/AA-00913/0/BIND-9-Security-Vulnerability-Matrix.html
URL	https://www.isc.org/software/bind

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the [ISC website](#).

3.1.27. PHP Vulnerability: CVE-2007-1581 (php-cve-2007-1581)

Description:

The resource system in PHP 5.0.0 through 5.2.1 allows context-dependent attackers to execute arbitrary code by interrupting the hash_update_file function via a userspace (1) error or (2) stream handler, which can then be used to destroy and modify internal resources. NOTE: it was later reported that PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 are also affected.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
BID	23062
CVE	CVE-2007-1581
XF	33248

Vulnerability Solution:

- Upgrade to PHP version 5.2.14

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.14.tar.gz>

- Upgrade to PHP version 5.3.2

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.2.tar.gz>

3.1.28. 'rexec' Remote Execution Service Enabled (service-rexec)

Description:

The RSH remote execution service (rexec) is enabled. This is a legacy service often configured to blindly trust some hosts and IPs. The protocol also doesn't support encryption or any sort of strong authentication mechanism.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:512	Running Remote Execution service

References:

None

Vulnerability Solution:

Disable or firewall this service which usually runs on 512/tcp.

3.1.29. USN-1013-1: FreeType vulnerabilities (ubuntu-usn-1013-1)

Description:

Integer overflow in base/ftstream.c in libXft (aka the X FreeType library) in FreeType before 2.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted Compact Font Format (CFF) font file that triggers a heap-based buffer overflow, related to an "input stream position error" issue, a different vulnerability than CVE-2010-1797.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libfreetype6 2.3.5-1ubuntu4.8.04.2

References:

Source	Reference
APPLE	APPLE-SA-2010-11-22-1
APPLE	APPLE-SA-2011-03-09-1

Source	Reference
APPLE	APPLE-SA-2011-03-09-3
APPLE	APPLE-SA-2011-03-21-1
APPLE	APPLE-SA-2011-07-15-1
APPLE	APPLE-SA-2011-07-15-2
BID	43700
BID	44214
BID	44643
CVE	CVE-2010-3311
CVE	CVE-2010-3814
CVE	CVE-2010-3855
DEBIAN	DSA-2116
DEBIAN	DSA-2155
REDHAT	RHSA-2010:0736
REDHAT	RHSA-2010:0737
REDHAT	RHSA-2010:0864
REDHAT	RHSA-2010:0889
USN	USN-1013-1

Vulnerability Solution:

- libfreetype6 on Ubuntu Linux 10.04

Upgrade libfreetype6 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

- libfreetype6 on Ubuntu Linux 10.10

Upgrade libfreetype6 for Ubuntu 10.10

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

- libfreetype6 on Ubuntu Linux 8.04

Upgrade libfreetype6 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

- libfreetype6 on Ubuntu Linux 9.10

Upgrade libfreetype6 for Ubuntu 9.10

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

3.1.30. USN-1085-1: tiff vulnerabilities (ubuntu-usn-1085-1)

Description:

Buffer overflow in Fax4Decode in LibTIFF 3.9.4 and possibly other versions, as used in ImageIO in Apple iTunes before 10.2 on Windows and other products, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a

crafted TIFF Internet Fax image file that has been compressed using CCITT Group 4 encoding, related to the EXPAND2D macro in libtiff/tif_fax3.h. NOTE: some of these details are obtained from third party information.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libtiff4 3.8.2-7ubuntu3.4

References:

Source	Reference
APPLE	APPLE-SA-2011-03-02-1
APPLE	APPLE-SA-2011-03-09-1
APPLE	APPLE-SA-2011-03-09-2
APPLE	APPLE-SA-2011-03-09-3
APPLE	APPLE-SA-2011-03-21-1
APPLE	APPLE-SA-2011-10-12-1
APPLE	APPLE-SA-2011-10-12-2
BID	46657
BID	46658
CVE	CVE-2010-2482
CVE	CVE-2010-2483
CVE	CVE-2010-2595
CVE	CVE-2010-2597
CVE	CVE-2010-2598
CVE	CVE-2010-2630
CVE	CVE-2010-3087
CVE	CVE-2011-0191
CVE	CVE-2011-0192
DEBIAN	DSA-2210
DEBIAN	DSA-2552
REDHAT	RHSA-2010:0519
REDHAT	RHSA-2010:0520
REDHAT	RHSA-2011:0318
USN	USN-1085-1

Vulnerability Solution:

•libtiff4 on Ubuntu Linux 10.04

Upgrade libtiff4 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

•libtiff4 on Ubuntu Linux 10.10

Upgrade libtiff4 for Ubuntu 10.10

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

•libtiff4 on Ubuntu Linux 8.04

Upgrade libtiff4 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

•libtiff4 on Ubuntu Linux 9.10

Upgrade libtiff4 for Ubuntu 9.10

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

3.1.31. USN-1153-1: libxml2 vulnerability (ubuntu-usn-1153-1)*Description:*

Integer overflow in xpath.c in libxml2 2.6.x through 2.6.32 and 2.7.x through 2.7.8, and libxml 1.8.16 and earlier, allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted XML file that triggers a heap-based buffer overflow when adding a new namespace node, related to handling of XPath expressions.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libxml2 2.6.31.dfsg-2ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2012-05-09-1
APPLE	APPLE-SA-2012-09-19-1
BID	48056
CVE	CVE-2011-1944
DEBIAN	DSA-2255
DISA_SEVERITY	Category I
DISA_VMSKEY	V0032171
DISA_VMSKEY	V0033884

Source	Reference
IAVM	2012-A-0073
IAVM	2012-A-0153
OSVDB	73248
REDHAT	RHSA-2011:1749
REDHAT	RHSA-2013:0217
USN	USN-1153-1

Vulnerability Solution:

- libxml2 on Ubuntu Linux 10.04
Upgrade libxml2 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libxml2 to the latest version
- libxml2 on Ubuntu Linux 10.10
Upgrade libxml2 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libxml2 to the latest version
- libxml2 on Ubuntu Linux 11.04
Upgrade libxml2 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade libxml2 to the latest version
- libxml2 on Ubuntu Linux 8.04
Upgrade libxml2 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libxml2 to the latest version

3.1.32. USN-1267-1: FreeType vulnerabilities (ubuntu-usn-1267-1)*Description:*

FreeType in CoreGraphics in Apple iOS before 5.0.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted font in a document.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libfreetype6 2.3.5-1ubuntu4.8.04.2

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-1
APPLE	APPLE-SA-2011-11-10-1

Source	Reference
APPLE	APPLE-SA-2012-02-01-1
BID	50155
CVE	CVE-2011-3256
CVE	CVE-2011-3439
DEBIAN	DSA-2328
USN	USN-1267-1
XF	70552

Vulnerability Solution:

•libfreetype6 on Ubuntu Linux 10.04

Upgrade libfreetype6 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

•libfreetype6 on Ubuntu Linux 10.10

Upgrade libfreetype6 for Ubuntu 10.10

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

•libfreetype6 on Ubuntu Linux 11.04

Upgrade libfreetype6 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

•libfreetype6 on Ubuntu Linux 11.10

Upgrade libfreetype6 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

•libfreetype6 on Ubuntu Linux 8.04

Upgrade libfreetype6 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

3.1.33. USN-1334-1: libxml2 vulnerabilities (ubuntu-usn-1334-1)*Description:*

Off-by-one error in libxml in Apple Safari before 5.0.6 allows remote attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow and application crash) via a crafted web site.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libxml2 2.6.31.dfsg-2ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2011-07-20-1
APPLE	APPLE-SA-2011-10-12-1
APPLE	APPLE-SA-2011-10-12-2
APPLE	APPLE-SA-2012-05-09-1
APPLE	APPLE-SA-2012-09-19-1
BID	51300
CVE	CVE-2011-0216
CVE	CVE-2011-2821
CVE	CVE-2011-2834
CVE	CVE-2011-3905
CVE	CVE-2011-3919
DEBIAN	DSA-2394
DISA_SEVERITY	Category I
DISA_VMSKEY	V0032171
DISA_VMSKEY	V0033884
IAVM	2012-A-0073
IAVM	2012-A-0153
OSVDB	75560
OVAL	OVAL13840
OVAL	OVAL14410
OVAL	OVAL14504
OVAL	OVAL14761
REDHAT	RHSA-2011:1749
REDHAT	RHSA-2013:0217
USN	USN-1334-1
XF	69885

Vulnerability Solution:

- libxml2 on Ubuntu Linux 10.04

Upgrade libxml2 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version

- libxml2 on Ubuntu Linux 10.10

Upgrade libxml2 for Ubuntu 10.10

Use `apt-get upgrade` to upgrade libxml2 to the latest version

- libxml2 on Ubuntu Linux 11.04

Upgrade libxml2 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libxml2 to the latest version

- libxml2 on Ubuntu Linux 11.10

Upgrade libxml2 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libxml2 to the latest version

- libxml2 on Ubuntu Linux 8.04

Upgrade libxml2 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version

3.1.34. USN-1357-1: OpenSSL vulnerabilities (ubuntu-usn-1357-1)

Description:

Double free vulnerability in OpenSSL 0.9.8 before 0.9.8s, when X509_V_FLAG_POLICY_CHECK is enabled, allows remote attackers to have an unspecified impact by triggering failure of a policy check.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu openssl 0.9.8g-4ubuntu3

References:

Source	Reference
APPLE	APPLE-SA-2013-06-04-1
BID	51563
CERT-VN	536044
CERT-VN	737740
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

Source	Reference
CVE	CVE-2012-0027
CVE	CVE-2012-0050
DEBIAN	DSA-2309
DEBIAN	DSA-2390
DEBIAN	DSA-2392
DISA_SEVERITY	Category I
DISA_VMSKEY	V0033794
DISA_VMSKEY	V0033884
DISA_VMSKEY	V0036639
IAVM	2012-A-0148
IAVM	2012-A-0153
IAVM	2013-A-0027
OSVDB	78191
OSVDB	78320
REDHAT	RHSA-2012:1306
REDHAT	RHSA-2012:1307
REDHAT	RHSA-2012:1308
USN	USN-1357-1
XF	72129

Vulnerability Solution:

- libssl0.9.8 on Ubuntu Linux 10.04
Upgrade libssl0.9.8 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libssl0.9.8 to the latest version
- libssl0.9.8 on Ubuntu Linux 10.10
Upgrade libssl0.9.8 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libssl0.9.8 to the latest version
- libssl0.9.8 on Ubuntu Linux 11.04
Upgrade libssl0.9.8 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade libssl0.9.8 to the latest version
- libssl0.9.8 on Ubuntu Linux 8.04
Upgrade libssl0.9.8 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libssl0.9.8 to the latest version
- libssl1.0.0 on Ubuntu Linux 11.10
Upgrade libssl1.0.0 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade libssl1.0.0 to the latest version

- openssl on Ubuntu Linux 10.04
Upgrade openssl for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade openssl to the latest version
- openssl on Ubuntu Linux 10.10
Upgrade openssl for Ubuntu 10.10
Use `apt-get upgrade` to upgrade openssl to the latest version
- openssl on Ubuntu Linux 11.04
Upgrade openssl for Ubuntu 11.04
Use `apt-get upgrade` to upgrade openssl to the latest version
- openssl on Ubuntu Linux 11.10
Upgrade openssl for Ubuntu 11.10
Use `apt-get upgrade` to upgrade openssl to the latest version
- openssl on Ubuntu Linux 8.04
Upgrade openssl for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade openssl to the latest version

3.1.35. USN-1397-1: MySQL vulnerabilities (ubuntu-usn-1397-1)

Description:

Multiple format string vulnerabilities in the dispatch_command function in libmysqld/sql_parse.cc in mysqld in MySQL 4.0.0 through 5.0.83 allow remote authenticated users to cause a denial of service (daemon crash) and possibly have unspecified other impact via format string specifiers in a database name in a (1) COM_CREATE_DB or (2) COM_DROP_DB request. NOTE: some of these details are obtained from third party information.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu mysql-server-5.0 5.0.51a-3ubuntu5

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
APPLE	APPLE-SA-2010-11-10-1
APPLE	APPLE-SA-2011-06-23-1
BID	26353
BID	31486
BID	35609

Source	Reference
BID	37640
BID	37943
BID	37974
BID	38043
BID	39543
BID	40257
BID	41198
BID	42596
BID	42598
BID	42599
BID	42625
BID	42633
BID	42638
BID	42646
BID	43676
BID	51503
BID	51506
BID	51509
BID	51510
BID	51513
BID	51514
BID	51515
BID	51516
BID	51518
BID	51524
BID	51526
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

Source	Reference
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

Source	Reference
CVE	CVE-2012-0117
CVE	CVE-2012-0118
CVE	CVE-2012-0119
CVE	CVE-2012-0120
CVE	CVE-2012-0484
CVE	CVE-2012-0485
CVE	CVE-2012-0486
CVE	CVE-2012-0487
CVE	CVE-2012-0488
CVE	CVE-2012-0489
CVE	CVE-2012-0490
CVE	CVE-2012-0491
CVE	CVE-2012-0492
CVE	CVE-2012-0493
CVE	CVE-2012-0494
CVE	CVE-2012-0495
CVE	CVE-2012-0496
DEBIAN	DSA-1413
DEBIAN	DSA-1662
DEBIAN	DSA-1783
DEBIAN	DSA-1997
DEBIAN	DSA-2143
OSVDB	55734
OSVDB	61956
OSVDB	78371
OSVDB	78372
OSVDB	78374
OSVDB	78375
OSVDB	78377
OSVDB	78378
OSVDB	78379
OSVDB	78383
OSVDB	78384

Source	Reference
OSVDB	78385
OSVDB	78386
OSVDB	78387
OSVDB	78388
OSVDB	78389
OSVDB	78390
OSVDB	78393
OSVDB	78394
OVAL	OVAL10258
OVAL	OVAL10521
OVAL	OVAL10591
OVAL	OVAL10846
OVAL	OVAL11116
OVAL	OVAL11349
OVAL	OVAL11390
OVAL	OVAL11456
OVAL	OVAL11857
OVAL	OVAL11869
OVAL	OVAL6693
OVAL	OVAL7210
OVAL	OVAL7328
OVAL	OVAL8156
OVAL	OVAL8500
OVAL	OVAL9490
REDHAT	RHSA-2007:1155
REDHAT	RHSA-2007:1157
REDHAT	RHSA-2009:1067
REDHAT	RHSA-2009:1289
REDHAT	RHSA-2010:0109
REDHAT	RHSA-2010:0110
REDHAT	RHSA-2010:0442
REDHAT	RHSA-2010:0824
REDHAT	RHSA-2010:0825

Source	Reference
REDHAT	RHSA-2011:0164
USN	USN-1397-1
XF	38284
XF	45042
XF	45590
XF	45649
XF	51614
XF	55416
XF	64683
XF	64684
XF	64685
XF	64686
XF	64687
XF	64688
XF	64838
XF	64839
XF	64840
XF	64841
XF	64842
XF	64843
XF	64844
XF	64845
XF	72518
XF	72519
XF	72520
XF	72521
XF	72525
XF	72526
XF	72527
XF	72528
XF	72529
XF	72530
XF	72531

Source	Reference
XF	72532
XF	72533
XF	72537
XF	72538
XF	72539
XF	72540

Vulnerability Solution:

- mysql-server-5.0 on Ubuntu Linux 8.04
Upgrade mysql-server-5.0 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade mysql-server-5.0 to the latest version
- mysql-server-5.1 on Ubuntu Linux 10.04
Upgrade mysql-server-5.1 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade mysql-server-5.1 to the latest version
- mysql-server-5.1 on Ubuntu Linux 10.10
Upgrade mysql-server-5.1 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade mysql-server-5.1 to the latest version
- mysql-server-5.1 on Ubuntu Linux 11.04
Upgrade mysql-server-5.1 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade mysql-server-5.1 to the latest version
- mysql-server-5.1 on Ubuntu Linux 11.10
Upgrade mysql-server-5.1 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade mysql-server-5.1 to the latest version

3.1.36. USN-1789-1: PostgreSQL vulnerabilities (ubuntu-usn-1789-1)*Description:*

PostgreSQL 9.2.x before 9.2.4, 9.1.x before 9.1.9, 9.0.x before 9.0.13, and 8.4.x before 8.4.17, when using OpenSSL, generates insufficiently random numbers, which might allow remote authenticated users to have an unspecified impact via vectors related to the "contrib/pgcrypto functions."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu postgresql-8.3 8.3.1-1

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
APPLE	APPLE-SA-2013-09-17-1
CVE	CVE-2013-1899
CVE	CVE-2013-1900
CVE	CVE-2013-1901
DEBIAN	DSA-2657
DEBIAN	DSA-2658
REDHAT	RHSA-2013:1475
USN	USN-1789-1

Vulnerability Solution:

- postgresql-8.3 on Ubuntu Linux 8.04
Upgrade postgresql-8.3 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version
- postgresql-8.4 on Ubuntu Linux 10.04
Upgrade postgresql-8.4 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version
- postgresql-9.1 on Ubuntu Linux 11.10
Upgrade postgresql-9.1 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade postgresql-9.1 to the latest version
- postgresql-9.1 on Ubuntu Linux 12.04
Upgrade postgresql-9.1 for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade postgresql-9.1 to the latest version
- postgresql-9.1 on Ubuntu Linux 12.10
Upgrade postgresql-9.1 for Ubuntu 12.10
Use `apt-get upgrade` to upgrade postgresql-9.1 to the latest version

3.1.37. USN-617-1: Samba vulnerabilities (ubuntu-usn-617-1)*Description:*

Stack-based buffer overflow in nmbd in Samba 3.0.0 through 3.0.26a, when configured as a Primary or Backup Domain controller, allows remote attackers to have an unknown impact via crafted GETDC mailslot requests, related to handling of GETDC logon server requests.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu samba 3.0.20-0.1ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2007-12-17
APPLE	APPLE-SA-2008-06-30
BID	26454
BID	29404
BID	31255
CERT	TA07-352A
CVE	CVE-2007-4572
CVE	CVE-2008-1105
DEBIAN	DSA-1409
DEBIAN	DSA-1590
OVAL	OVAL10020
OVAL	OVAL11132
OVAL	OVAL5643
OVAL	OVAL5733
REDHAT	RHSA-2007:1013
REDHAT	RHSA-2007:1016
REDHAT	RHSA-2007:1017
REDHAT	RHSA-2008:0288
REDHAT	RHSA-2008:0289
REDHAT	RHSA-2008:0290
SUSE	SUSE-SA:2007:065
SUSE	SUSE-SA:2008:026
USN	USN-617-1
XF	38501
XF	42664
XF	45251

Vulnerability Solution:

•libsmbclient on Ubuntu Linux 7.04

Upgrade libsmbclient for Ubuntu 7.04

Use `apt-get upgrade` to upgrade libsmbclient to the latest version

•libsmbclient on Ubuntu Linux 7.10

Upgrade libsmbclient for Ubuntu 7.10

Use `apt-get upgrade` to upgrade libsmbclient to the latest version

•libsmbclient on Ubuntu Linux 8.04

Upgrade libsmbclient for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libsmbclient to the latest version

•samba on Ubuntu Linux 7.04

Upgrade samba for Ubuntu 7.04

Use `apt-get upgrade` to upgrade samba to the latest version

•samba on Ubuntu Linux 7.10

Upgrade samba for Ubuntu 7.10

Use `apt-get upgrade` to upgrade samba to the latest version

•samba on Ubuntu Linux 8.04

Upgrade samba for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade samba to the latest version

3.1.38. USN-839-1: Samba vulnerabilities (ubuntu-usn-839-1)

Description:

Multiple format string vulnerabilities in client/client.c in smbclient in Samba 3.2.0 through 3.2.12 might allow context-dependent attackers to execute arbitrary code via format string specifiers in a filename.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu samba 3.0.20-0.1ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2009-09-10-2
APPLE	APPLE-SA-2010-03-29-1
BID	35472
BID	36363
BID	36572

Source	Reference
BID	36573
CVE	CVE-2009-1886
CVE	CVE-2009-1888
CVE	CVE-2009-2813
CVE	CVE-2009-2906
CVE	CVE-2009-2948
DEBIAN	DSA-1823
OSVDB	57955
OSVDB	58519
OSVDB	58520
OVAL	OVAL10434
OVAL	OVAL10790
OVAL	OVAL7087
OVAL	OVAL7090
OVAL	OVAL7211
OVAL	OVAL7257
OVAL	OVAL7292
OVAL	OVAL7791
OVAL	OVAL9191
OVAL	OVAL9944
USN	USN-839-1
XF	51327
XF	51328
XF	53174
XF	53574
XF	53575

Vulnerability Solution:

- samba on Ubuntu Linux 8.04

Upgrade samba for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade samba to the latest version

- samba on Ubuntu Linux 8.10

Upgrade samba for Ubuntu 8.10

Use `apt-get upgrade` to upgrade samba to the latest version

- samba on Ubuntu Linux 9.04

Upgrade samba for Ubuntu 9.04

Use `apt-get upgrade` to upgrade samba to the latest version

- smbclient on Ubuntu Linux 8.10

Upgrade smbclient for Ubuntu 8.10

Use `apt-get upgrade` to upgrade smbclient to the latest version

- smbfs on Ubuntu Linux 8.04

Upgrade smbfs for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade smbfs to the latest version

- smbfs on Ubuntu Linux 8.10

Upgrade smbfs for Ubuntu 8.10

Use `apt-get upgrade` to upgrade smbfs to the latest version

- smbfs on Ubuntu Linux 9.04

Upgrade smbfs for Ubuntu 9.04

Use `apt-get upgrade` to upgrade smbfs to the latest version

3.1.39. USN-897-1: MySQL vulnerabilities (ubuntu-usn-897-1)

Description:

Multiple format string vulnerabilities in the dispatch_command function in libmysqld/sql_parse.cc in mysqld in MySQL 4.0.0 through 5.0.83 allow remote authenticated users to cause a denial of service (daemon crash) and possibly have unspecified other impact via format string specifiers in a database name in a (1) COM_CREATE_DB or (2) COM_DROP_DB request. NOTE: some of these details are obtained from third party information.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu mysql-server-5.0 5.0.51a-3ubuntu5

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
BID	31486
BID	35609
BID	37640
BID	37943
BID	37974

Source	Reference
BID	38043
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
DEBIAN	DSA-1662
DEBIAN	DSA-1783
DEBIAN	DSA-1997
OSVDB	55734
OSVDB	61956
OVAL	OVAL10591
OVAL	OVAL11116
OVAL	OVAL11349
OVAL	OVAL11456
OVAL	OVAL11857
OVAL	OVAL8156
OVAL	OVAL8500
REDHAT	RHSA-2009:1067
REDHAT	RHSA-2009:1289
REDHAT	RHSA-2010:0109
REDHAT	RHSA-2010:0110
USN	USN-897-1
XF	45590
XF	45649
XF	51614
XF	55416

Vulnerability Solution:

•mysql-server-5.0 on Ubuntu Linux 8.04

Upgrade mysql-server-5.0 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade mysql-server-5.0 to the latest version

- mysql-server-5.0 on Ubuntu Linux 8.10

Upgrade mysql-server-5.0 for Ubuntu 8.10

Use `apt-get upgrade` to upgrade mysql-server-5.0 to the latest version

- mysql-server-5.0 on Ubuntu Linux 9.04

Upgrade mysql-server-5.0 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade mysql-server-5.0 to the latest version

- mysql-server-5.1 on Ubuntu Linux 9.10

Upgrade mysql-server-5.1 for Ubuntu 9.10

Use `apt-get upgrade` to upgrade mysql-server-5.1 to the latest version

3.1.40. USN-972-1: FreeType vulnerabilities (ubuntu-usn-972-1)

Description:

Multiple stack-based buffer overflows in the cff_decoder_parse_charstrings function in the CFF Type2 CharStrings interpreter in cff/cffgload.c in FreeType before 2.4.2, as used in Apple iOS before 4.0.2 on the iPhone and iPod touch and before 3.2.2 on the iPad, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted CFF opcodes in embedded fonts in a PDF document, as demonstrated by JailbreakMe. NOTE: some of these details are obtained from third party information.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libfreetype6 2.3.5-1ubuntu4.8.04.2

References:

Source	Reference
APPLE	APPLE-SA-2010-08-11-1
APPLE	APPLE-SA-2010-08-11-2
APPLE	APPLE-SA-2010-11-10-1
APPLE	APPLE-SA-2010-11-22-1
BID	42151
BID	42285
CVE	CVE-2010-1797
CVE	CVE-2010-2541
CVE	CVE-2010-2805
CVE	CVE-2010-2806

Source	Reference
CVE	CVE-2010-2807
CVE	CVE-2010-2808
OSVDB	66828
REDHAT	RHSA-2010:0577
REDHAT	RHSA-2010:0578
REDHAT	RHSA-2010:0736
REDHAT	RHSA-2010:0737
REDHAT	RHSA-2010:0864
USN	USN-972-1
XF	60856

Vulnerability Solution:

- libfreetype6 on Ubuntu Linux 10.04

Upgrade libfreetype6 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

- libfreetype6 on Ubuntu Linux 8.04

Upgrade libfreetype6 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

- libfreetype6 on Ubuntu Linux 9.04

Upgrade libfreetype6 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

- libfreetype6 on Ubuntu Linux 9.10

Upgrade libfreetype6 for Ubuntu 9.10

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

3.1.41. Apache Tomcat Example Scripts Information Leakage (apache-tomcat-example-leaks)

Description:

The following example scripts that come with Apache Tomcat v4.x - v7.x and can be used by attackers to gain information about the system. These scripts are also known to be vulnerable to cross site scripting (XSS) injection.

- /examples/jsp/num/numguess.jsp

- /examples/jsp/dates/date.jsp

- /examples/jsp/snp/snoop.jsp

- /examples/jsp/error/error.html

- /examples/jsp/sessions/carts.html

- /examples/jsp/checkbox/check.html

- /examples/jsp/colors/colors.html

- /examples/jsp/cal/login.html
- /examples/jsp/include/include.jsp
- /examples/jsp/forward/forward.jsp
- /examples/jsp/plugin/plugin.jsp
- /examples/jsp/jsptoserv/jsptoservlet.jsp
- /examples/jsp/simpletag/foo.jsp
- /examples/jsp/mail/sendmail.jsp
- /examples/servlet/HelloWorldExample
- /examples/servlet/RequestInfoExample
- /examples/servlet/RequestHeaderExample
- /examples/servlet/RequestParamExample
- /examples/servlet/CookieExample
- /examples/servlet/JndiServlet
- /examples/servlet/SessionExample
- /tomcat-docs/appdev/sample/web/hello.jsp

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:8180	<p>Running HTTP serviceProduct Tomcat exists -- Apache TomcatHTTP GET request to http://192.168.0.102:8180/tomcat-docs/appdev/sample/web/hello.jsp HTTP response code was an expected 200</p> <p>19: limitations under the License.</p> <p>20: --></p> <p>21: <html></p> <p>22: <head></p> <p>19: <title>Sample Application JSP Page</title></p>

References:

None

Vulnerability Solution:

Delete these scripts entirely. Example scripts should never be installed on production servers.

3.1.42. VNC remote control service installed (backdoor-vnc-0001)

Description:

AT&T Virtual Network Computing (VNC) provides remote users with access to the system it is installed on. If this service is compromised, the user can gain complete control of the system.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:5900	Running VNC service

References:

None

Vulnerability Solution:

Remove or disable this service. If it is necessary, be sure to use well thought out (hard to crack) passwords. It is important to note that VNC [truncates passwords to 8 bytes](#) when authenticating, making it more susceptible to brute force attacks.

To protect data from eaves-droppers, [tunneling VNC through SSH](#) is recommended.

Additionally, restricting access to specific IP addresses [using TCP wrappers](#) is also recommended.

For more information on VNC, visit the [VNC website](#).

3.1.43. CIFS NULL Session Permitted (cifs-nt-0001)*Description:*

NULL sessions allow anonymous users to establish unauthenticated CIFS sessions with Windows or third-party CIFS implementations such as [Samba](#) or the [Solaris CIFS Server](#). These anonymous users may be able to enumerate local users, groups, servers, shares, domains, domain policies, and may be able to access various MSRPC services through RPC function calls. These services have been historically affected by numerous vulnerabilities. The wealth of information available to attackers through NULL sessions may also allow them to carry out more sophisticated attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Found server name: METASPLOITABLE Found policy for domain(s): METASPLOITABLE Builtin

References:

Source	Reference
CVE	CVE-1999-0519
URL	http://www.hsc.fr/ressources/presentations/null_sessions/

Vulnerability Solution:

•Microsoft Windows 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003

Disable NULL sessions for Windows 2003

Modify the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\

with the following values:

Value Name: RestrictAnonymous

Data Type: REG_DWORD

Data Value: 1

Value Name: RestrictAnonymousSAM

Data Type: REG_DWORD

Data Value: 1

Value Name: EveryoneIncludesAnonymous

Data Type: REG_DWORD

Data Value: 0

and set the following value to 0 (or, alternatively, delete it):

Value Name: TurnOffAnonymousBlock

Data Type: REG_DWORD

Data Value: 0

Modify the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\

with the following values:

Value Name: RestrictNullSessAccess

Data Type: REG_DWORD

Data Value: 1

Value Name: NullSessionPipes

Data Type: REG_MULTI_SZ

Data Value: "" (empty string, without quotes)

Open Local Security Settings, and disable the following setting:

Security Settings -> Local Policies -> Security Options ->

Network access: Allow anonymous SID/Name translation: Disabled

Finally, reboot the machine.

Please note that disabling NULL sessions may have an adverse impact on functionality, as some applications and network environments may depend on them for proper operation. Refer to [Microsoft Knowledge Base Article 823659](#) for more information.

•Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional

Disable NULL sessions for Windows XP

Modify the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\

with the following values:

Value Name: RestrictAnonymous

Data Type: REG_DWORD

Data Value: 1

Value Name: RestrictAnonymousSAM

Data Type: REG_DWORD

Data Value: 1

Value Name: EveryoneIncludesAnonymous

Data Type: REG_DWORD

Data Value: 0

Modify the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\

with the following values:

Value Name: RestrictNullSessAccess

Data Type: REG_DWORD

Data Value: 1

Value Name: NullSessionPipes

Data Type: REG_MULTI_SZ

Data Value: "" (empty string, without quotes)

Open Local Security Settings, and disable the following setting:

Security Settings -> Local Policies -> Security Options ->

Network access: Allow anonymous SID/Name translation: Disabled

Finally, reboot the machine.

Please note that disabling NULL sessions may have an adverse impact on functionality, as some applications and network environments may depend on them for proper operation. Refer to [Microsoft Knowledge Base Article Q246261](#) for more information.

- Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server

Disable NULL sessions for Windows 2000

Modify the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\

with the following value:

Value Name: RestrictAnonymous

Data Type: REG_DWORD

Data Value: 2

After modifying the registry, reboot the machine.

Please note that disabling NULL sessions may have an adverse impact on functionality, as some applications and network environments may depend on them for proper operation. Refer to [Microsoft Knowledge Base Article Q246261](https://support.microsoft.com/kb/q246261) for more information.

- Microsoft Windows NT Server 4.0, Microsoft Windows NT Server, Enterprise Edition 4.0, Microsoft Windows NT Workstation 4.0

Install Microsoft service pack Windows NT4 Service Pack 4

Download and apply the upgrade from: <http://support.microsoft.com/sp>

- Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition

Disable NULL sessions for Windows NT

Modify the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\

with the following value:

Value Name: RestrictAnonymous

Data Type: REG_DWORD

Data Value: 1

After modifying the registry, reboot the machine.

It is important to note that on Windows NT 4.0 systems, setting this registry entry will still leave the system open to various attacks, including brute-force enumeration of users and groups. A complete solution for Windows NT 4.0 systems is not available.

- Samba on Linux

Restrict anonymous access

To restrict anonymous access to Samba, modify your "smb.conf" settings as follows:

```
guest account = nobody
```

```
restrict anonymous = 1
```

Note: Make sure you do NOT list a user "nobody" in your password file.

- Novell NetWare

Novell Netware CIFS

As of May 9, 2007 Novell Netware CIFS does not provide a workaround for this vulnerability.

3.1.44. Samba AFS Filesystem ACL Mapping Format String Vulnerability (cifs-samba-afs-filesystem-acl-mapping-bof)

Description:

Format string vulnerability in the afsacl.so VFS module in Samba 3.0.6 through 3.0.23d allows context-dependent attackers to execute arbitrary code via format string specifiers in a filename on an AFS file system, which is not properly handled during Windows ACL mapping.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:139	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian
192.168.0.102:445	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian

References:

Source	Reference
BID	22403
CERT-VN	649732
CVE	CVE-2007-0454
DEBIAN	DSA-1257
OSVDB	33101
URL	http://www.samba.org/samba/security/CVE-2007-0454.html
XF	32304

Vulnerability Solution:

Samba < 3.0.24

Download and apply the upgrade from: <https://ftp.samba.org/pub/samba/stable/samba-3.0.24.tar.gz>

Alternatively, patches may be available at <http://www.samba.org/samba/history/security.html>. Although Samba provides source code, it is recommended that you use your operating system's package manager to upgrade if possible. Please note that many operating system vendors choose to apply the most recent Samba security patches to their distributions without changing the package version to the most recent Samba version number. For the most reliable scan results, use correlation with authenticated scans.

3.1.45. ISC BIND: A specially crafted Resource Record could cause named to terminate (CVE-2012-4244) (dns-bind-cve-2012-4244)

Description:

ISC BIND 9.x before 9.7.6-P3, 9.8.x before 9.8.3-P3, 9.9.x before 9.9.1-P3, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P3 allows remote attackers to cause a denial of service (assertion failure and named daemon exit) via a query for a long resource record.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of

Affected Nodes:	Additional Information:
	product BIND found -- BIND 9.4.2

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CVE	CVE-2012-4244
DEBIAN	DSA-2547
DISA_SEVERITY	Category I
DISA_VMSKEY	V0036787
IAVM	2013-A-0031
REDHAT	RHSA-2012:1266
REDHAT	RHSA-2012:1267
REDHAT	RHSA-2012:1268
REDHAT	RHSA-2012:1365
URL	https://kb.isc.org/article/AA-00778/0
URL	https://kb.isc.org/article/AA-00778/74/CVE-2012-4244%3A-A-specially-crafted-Resource-Record-could-cause-named-to-terminate.html

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the [ISC website](#).

3.1.46. IP Source Routing Enabled (generic-ip-source-routing-enabled)*Description:*

The host is configured to honor IP source routing options. Source routing is a feature of the IP protocol which allows the sender of a packet to specify which route the packet should take on the way to its destination (and on the way back). Source routing was originally designed to be used when a host did not have proper default routes in its routing table. However, source routing is rarely used for legitimate purposes nowadays. Attackers can abuse source routing to bypass firewalls or to map your network.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	The net.ipv4.conf.all.accept_source_route sysctl variable is set to 0, as expected. The net.ipv4.conf.all.forwarding sysctl variable is set to 0, as expected. The net.ipv4.conf.all.mc_forwarding sysctl variable is set to 0, as expected. The net.ipv4.conf.default.accept_source_route sysctl variable is set to 1, expected 0. The net.ipv4.conf.default.forwarding sysctl variable is set to 0, as expected. The net.ipv4.conf.default.mc_forwarding sysctl variable is set to 0, as expected.

References:

Source	Reference
BID	646
CVE	CVE-1999-0510
CVE	CVE-1999-0909
MS	MS99-038
MSKB	238453
URL	http://packetstormsecurity.nl/advisories/nai/nai.99-09-20.windows_ip_source_routing

Vulnerability Solution:

•IBM AIX

Disable IP source routing on IBM AIX

Issue the following command to disable forwarding of source routed packets:

```
/usr/sbin/no -o nonlocsrcroute=0
```

Also, issue the following command to disable the sending of source routed packets:

```
/usr/sbin/no -o ipsrctestsend=0
```

In order to make this setting permanent, you can add this command to /etc/rc.net.

You should also consider blocking or "scrubbing" source routed packets at your firewall (i.e. either reject source routed packets or have the firewall remove the source routing options if possible).

•FreeBSD

Disable IP source routing on FreeBSD

IP source routing is disabled by default. Confirm that the 'net.inet.ip.sourceroute' sysctl option is set to 0 by issuing the following command:

```
sysctl net.inet.ip.sourceroute
```

If the option is not set to 0, you can set it to zero by issuing the following command:

```
sysctl -w net.inet.ip.sourceroute=0
```

These settings can be added to /etc/sysctl.conf to make them permanent.

You should also consider blocking or "scrubbing" source routed packets at your firewall (i.e. either reject source routed packets or have the firewall remove the source routing options if possible).

•Cisco IOS

Disable IP source routing on Cisco IOS

Use the 'no ip source-route' command to disable source-routing on the affected interface(s).

You should also consider blocking or "scrubbing" source routed packets at your firewall (i.e. either reject source routed packets or have the firewall remove the source routing options if possible).

•SGI Irix

Disable IP source routing on SGI Irix

Issue the following command to disable forwarding of source routed packets:

`/usr/sbin/systune ipforward to 2`

You should also consider blocking or "scrubbing" source routed packets at your firewall (i.e. either reject source routed packets or have the firewall remove the source routing options if possible).

•Linux

Disable IP source routing on Linux

Source routing is disabled by default. On Linux kernel 2.2 and earlier, this setting was controlled by the contents of the following proc file:

`/proc/sys/net/ipv4/conf/all/accept_source_route`

However, in more recent versions of Linux, the source route setting is controlled by several sysctl variables. Issue the following command to drop all source routed packets:

`/sbin/sysctl -w net.ipv4.conf.all.accept_source_route=0`

Also, issue the following commands to disable forwarding of any frames with source routing options:

`/sbin/sysctl -w net.ipv4.conf.all.forwarding=0`

`/sbin/sysctl -w net.ipv4.conf.all.mc_forwarding=0`

These settings can be added to `/etc/sysctl.conf` to make them permanent.

You should also consider blocking or "scrubbing" source routed packets at your firewall (i.e. either reject source routed packets or have the firewall remove the source routing options if possible).

•Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition

Disable IP source routing on Windows NT 4

First upgrade to the [latest NT4 Service Pack](#) (SP6 for NT4 Terminal Server, SP6a for all other versions of NT4). Versions of NT4 prior to SP6 can still be "tricked" into honoring source routing even if you have disabled it via the registry. See [Q238453](#) for more information.

After upgrading to NT Service Pack 6a, run the registry editor (regedit.exe) and browse to the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Add a DWORD value named "DisableIPSourceRouting", and set it to 2. Windows must be rebooted for the change to take effect.

You should also consider blocking or "scrubbing" source routed packets at your firewall (i.e. either reject source routed packets or have the firewall remove the source routing options if possible).

•OpenBSD

Disable IP source routing on OpenBSD

IP source routing is disabled by default. Confirm that the 'net.inet.ip.sourceroute' sysctl option is set to 0 by issuing the following command:

`sysctl net.inet.ip.sourceroute`

If the option is not set to 0, you can set it to zero by issuing the following command:

`sysctl -w net.inet.ip.sourceroute=0`

These settings can be added to `/etc/sysctl.conf` to make them permanent.

You should also consider blocking or "scrubbing" source routed packets at your firewall (i.e. either reject source routed packets or have the firewall remove the source routing options if possible).

•Cisco PIX

Disable IP source routing on Cisco PIX

PIX firewalls are designed to drop IP packets with insecure options, including source routing. See the following [Cisco support document](#) for more information.

You should also consider blocking or "scrubbing" source routed packets at your firewall (i.e. either reject source routed packets or have the firewall remove the source routing options if possible).

•Sun Solaris

Disable IP source routing on Solaris

While you cannot completely disable Solaris's handling of source-routed packets directed at the Solaris host itself, you can prevent Solaris from forwarding source routed packets on to the next hop by issuing the following command:

```
/usr/sbin/ndd -set /dev/ip ip_forward_src_routed 0
```

In order to make this setting permanent, you will need to set this option automatically when the machine is booted.

You should also consider blocking or "scrubbing" source routed packets at your firewall (i.e. either reject source routed packets or have the firewall remove the source routing options if possible).

•Microsoft Windows Vista, Microsoft Windows Vista Home, Basic Edition, Microsoft Windows Vista Home, Basic N Edition, Microsoft Windows Vista Home, Premium Edition, Microsoft Windows Vista Ultimate Edition, Microsoft Windows Vista Enterprise Edition, Microsoft Windows Vista Business Edition, Microsoft Windows Vista Business N Edition, Microsoft Windows Vista Starter Edition, Microsoft Windows Server 2008, Microsoft Windows Server 2008 Standard Edition, Microsoft Windows Server 2008 Enterprise Edition, Microsoft Windows Server 2008 Datacenter Edition, Microsoft Windows Server 2008 HPC Edition, Microsoft Windows Server 2008 Web Edition, Microsoft Windows Server 2008 Storage Edition, Microsoft Windows Small Business Server 2008, Microsoft Windows Essential Business Server 2008, Microsoft Windows Server 2012, Microsoft Windows Server 2012 Essentials Edition, Microsoft Windows Server 2012 Standard Edition, Microsoft Windows Server 2012 Datacenter Edition, Microsoft Windows Server 2012 Foundation Edition, Microsoft Windows Storage Server 2012, Microsoft Windows 7, Microsoft Windows 7 Home, Basic Edition, Microsoft Windows 7 Home, Basic N Edition, Microsoft Windows 7 Home, Premium Edition, Microsoft Windows 7 Home, Premium N Edition, Microsoft Windows 7 Ultimate Edition, Microsoft Windows 7 Ultimate N Edition, Microsoft Windows 7 Enterprise Edition, Microsoft Windows 7 Enterprise N Edition, Microsoft Windows 7 Professional Edition, Microsoft Windows 7 Starter Edition, Microsoft Windows 7 Starter N Edition, Microsoft Windows Embedded Standard 7, Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 R2, Enterprise Edition, Microsoft Windows Server 2008 R2, Standard Edition, Microsoft Windows Server 2008 R2, Datacenter Edition, Microsoft Windows Server 2008 R2, Web Edition, Microsoft Windows 8, Microsoft Windows 8 Enterprise Edition, Microsoft Windows 8 Professional Edition, Microsoft Windows RT

Disable IP source routing on Windows Vista and newer

Run the registry editor (regedit.exe) and browse to the following keys:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters

For Tcpip, the DWORD value named "DisableIPSourceRouting" must either not exist or have a value of 1 or 2. For Tcpip6, the DWORD value named "DisableIPSourceRouting" must exist and have a value of 1 or 2. For the highest security level, both should exist and be set to 2. Windows must be rebooted for the change to take effect.

You should also consider blocking or "scrubbing" source routed packets at your firewall (i.e. either reject source routed packets or have the firewall remove the source routing options if possible).

See [_](#)

<http://technet.microsoft.com/library/dd349797%28v=ws.10%29.aspx> for more information.

- Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server, Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003

Disable IP source routing on Windows 2000/XP/2003

Run the registry editor (regedit.exe) and browse to the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Add a DWORD value named "DisableIPSourceRouting", and set it to 2. Windows must be rebooted for the change to take effect.

You should also consider blocking or "scrubbing" source routed packets at your firewall (i.e. either reject source routed packets or have the firewall remove the source routing options if possible).

- Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows 98SE, Microsoft Windows ME

Disable IP source routing on Windows 95/98/ME

Microsoft has provided a fix for this issue, but requires users to contact Microsoft directly to obtain the fix. Please see MSKB article [Q238453](#) for more information.

You should also consider blocking or "scrubbing" source routed packets at your firewall (i.e. either reject source routed packets or have the firewall remove the source routing options if possible).

3.1.47. PHP Multiple Vulnerabilities Fixed in version 5.2.11 (<http-php-multiple-vulns-5-2-11>)

Description:

Unspecified vulnerability in the imagecolortransparent function in PHP before 5.2.11 has unknown impact and attack vectors related to an incorrect "sanity check for the color index."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
CVE	CVE-2009-3291
CVE	CVE-2009-3292
CVE	CVE-2009-3293

Source	Reference
DEBIAN	DSA-1940
OSVDB	58185
OSVDB	58186
OSVDB	58187
OVAL	OVAL10438
OVAL	OVAL7047
OVAL	OVAL7394
OVAL	OVAL7652
OVAL	OVAL9982
URL	http://bugs.php.net/44683
URL	http://www.php.net/ChangeLog-5.php#5.2.11
URL	http://www.php.net/releases/5_2_11.php
XF	53334

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.11.tar.gz>

3.1.48. PHP Multiple Vulnerabilities Fixed in version 5.3.1 (http-php-multiple-vulns-5-3-1)*Description:*

**** DISPUTED **** main/streams/plain_wrapper.c in PHP 5.3.x before 5.3.1 does not recognize the `safe_mode_include_dir` directive, which allows context-dependent attackers to have an unknown impact by triggering the failure of PHP scripts that perform include or require operations, as demonstrated by a script that attempts to perform a `require_once` on a file in a standard library directory. NOTE: a reliable third party reports that this is not a vulnerability, because it results in a more restrictive security policy.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
APPLE	APPLE-SA-2010-03-29-1
CVE	CVE-2009-3292
CVE	CVE-2009-3557

Source	Reference
CVE	CVE-2009-3558
CVE	CVE-2009-3559
CVE	CVE-2009-4017
DEBIAN	DSA-1940
OSVDB	58186
OVAL	OVAL10483
OVAL	OVAL6667
OVAL	OVAL7396
OVAL	OVAL7652
OVAL	OVAL9982
URL	http://www.php.net/ChangeLog-5.php#5.3.1
URL	http://www.php.net/releases/5_3_1.php
XF	54455

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.1.tar.gz>

3.1.49. MySQL default account: root/no password (mysql-default-account-root-nopassword)*Description:*

The default configuration of the Windows binary release of MySQL 3.23.2 through 3.23.52 has a NULL root password, which could allow remote attackers to gain unauthorized root access to the MySQL database.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceSuccessfully authenticated to the MySQL service with credentials: uid[root] pw[] realm[mysql]

References:

Source	Reference
BID	5503
CVE	CVE-2002-1809
XF	9902

Vulnerability Solution:

The password should be changed to a non-default value. To change the password for the account, use the mysql command line tool to run the commands:


```
UPDATE user SET password=password('new-password') WHERE user='user-name';
FLUSH PRIVILEGES;
```

Where user-name should be replaced with the appropriate user name and new-password should be replaced with the new password.

3.1.50. Debian's OpenSSL Library Predictable Random Number Generator (openssl-debian-weak-keys)

Description:

A weakness has been discovered in the random number generator used by OpenSSL on Debian and Ubuntu systems. As a result of this weakness, certain encryption keys are much more common than they should be, such that an attacker could guess the key through a brute-force attack given minimal knowledge of the system. This particularly affects the use of encryption keys in OpenSSH, OpenVPN and SSL certificates. This vulnerability only affects operating systems which are based on Debian. However, other systems can be indirectly affected if weak keys are imported into them.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:22	SSH public key with fingerprint 5656240F211DDEA72BAE61B1243DE8F3 is a known weak key

References:

Source	Reference
BID	29179
CERT	TA08-137A
CERT-VN	925211
CVE	CVE-2008-0166
DEBIAN	DSA-1571
DEBIAN	DSA-1576
URL	http://metasploit.com/users/hdm/tools/debian-openssl/
URL	http://wiki.debian.org/SSLkeys
URL	http://www.debian.org/security/2008/dsa-1571
URL	http://www.debian.org/security/2008/dsa-1576
URL	http://www.debian.org/security/key-rollover/
URL	http://www.ubuntu.com/usn/usn-612-1
URL	http://www.ubuntu.com/usn/usn-612-2
URL	http://www.ubuntu.com/usn/usn-612-3
URL	http://www.ubuntu.com/usn/usn-612-4

Source	Reference
URL	http://www.ubuntu.com/usn/usn-612-5
URL	http://www.ubuntu.com/usn/usn-612-6
URL	http://www.ubuntu.com/usn/usn-612-7
URL	http://www.ubuntu.com/usn/usn-612-8
XF	42375

Vulnerability Solution:

Upgrade the OpenSSL package to the version recommended below to fix the random number generator and stop generating weak keys

- For Debian 4.0 etch, upgrade to 0.9.8c-4etch3
- For Debian testing (lenny), upgrade to 0.9.8g-9
- For Debian unstable (sid), upgrade to 0.9.8g-9
- For Ubuntu 7.0.4 (feisty), upgrade to 0.9.8c-4ubuntu0.3
- For Ubuntu 7.10 (gusty), upgrade to 0.9.8e-5ubuntu3.2
- For Ubuntu 8.0.4 (hardy), upgrade to 0.9.8g-4ubuntu3.1

Then regenerate all cryptographic key material which has been created by vulnerable OpenSSL versions on Debian-based systems.

Affected keys include SSH server and user keys, OpenVPN keys, DNSSEC keys, keys associated to X.509 certificates, etc.

Optionally, Debian and Ubuntu have released updated OpenSSH, OpenSSL and OpenVPN packages to automatically blacklist known weak keys. It is recommended to install these upgrades on all systems.

3.1.51. PHP Vulnerability: CVE-2007-4825 (php-cve-2007-4825)*Description:*

Directory traversal vulnerability in PHP 5.2.4 and earlier allows attackers to bypass open_basedir restrictions and possibly execute arbitrary code via a .. (dot dot) in the dl function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2007-4825
OSVDB	45902
SUSE	SUSE-SA:2008:004
XF	36528

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.5.tar.gz>

3.1.52. PHP Vulnerability: CVE-2012-2386 (php-cve-2012-2386)*Description:*

Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
CVE	CVE-2012-2386

Vulnerability Solution:

- Upgrade to PHP version 5.3.14

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 5.4.4

Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.53. PHP Vulnerability: CVE-2013-1635 (php-cve-2013-1635)*Description:*

ext/soap/soap.c in PHP before 5.3.22 and 5.4.x before 5.4.13 does not validate the relationship between the soap.wsdl_cache_dir directive and the open_basedir directive, which allows remote attackers to bypass intended access restrictions by triggering the creation of cached SOAP WSDL files in an arbitrary directory.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CVE	CVE-2013-1635
DEBIAN	DSA-2639

Vulnerability Solution:

- Upgrade to PHP version 5.3.22

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 5.4.13

Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.54. PHP Vulnerability: CVE-2014-8626 (php-cve-2014-8626)*Description:*

Stack-based buffer overflow in the date_from_ISO8601 function in ext/xmlrpc/libxmlrpc/xmlrpc.c in PHP before 5.2.7 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code by including a timezone field in a date, leading to improper XML-RPC encoding.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2014-8626
REDHAT	RHSA-2014:1824
REDHAT	RHSA-2014:1825

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.7.tar.gz>

3.1.55. PHP Vulnerability: CVE-2014-9425 (php-cve-2014-9425)*Description:*

Double free vulnerability in the zend_ts_hash_graceful_destroy function in zend_ts_hash.c in the Zend Engine in PHP through 5.5.20 and 5.6.x through 5.6.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2014-9425
URL	https://bugs.php.net/bug.php?id=68676

Vulnerability Solution:

- Upgrade to PHP version 5.5.21

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 5.6.5

Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.56. PHP Vulnerability: CVE-2014-9426 (php-cve-2014-9426)*Description:*

**** DISPUTED **** The apprentice_load function in libmagic/apprentice.c in the Fileinfo component in PHP through 5.6.4 attempts to perform a free operation on a stack-based character array, which allows remote attackers to cause a denial of service (memory corruption or application crash) or possibly have unspecified other impact via unknown vectors. NOTE: this is disputed by the vendor because the standard erealloc behavior makes the free operation unreachable.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2014-9426
URL	https://bugs.php.net/bug.php?id=68665

Vulnerability Solution:

Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.57. PHP Vulnerability: CVE-2014-9653 (php-cve-2014-9653)

Description:

readelf.c in file before 5.22, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not consider that pread calls sometimes read only a subset of the available data, which allows remote attackers to cause a denial of service (uninitialized memory access) or possibly have unspecified other impact via a crafted ELF file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2014-9653
DEBIAN	DSA-3196

Vulnerability Solution:

- Upgrade to PHP version 5.4.37
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.5.21
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.6.5
Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.58. PHP Vulnerability: CVE-2014-9705 (php-cve-2014-9705)

Description:

Heap-based buffer overflow in the enchant_broker_request_dict function in ext/enchant/enchant.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allows remote attackers to execute arbitrary code via vectors that trigger creation of multiple dictionaries.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
--------	-----------

Source	Reference
CVE	CVE-2014-9705
DEBIAN	DSA-3195

Vulnerability Solution:

- Upgrade to PHP version 5.4.38
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.5.22
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.6.6
Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.59. PHP Vulnerability: CVE-2015-0273 (php-cve-2015-0273)*Description:*

Multiple use-after-free vulnerabilities in ext/date/php_date.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allow remote attackers to execute arbitrary code via crafted serialized input containing a (1) R or (2) r type specifier in (a) DateTimeZone data handled by the php_date_timezone_initialize_from_hash function or (b) DateTime data handled by the php_date_initialize_from_hash function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2015-0273
DEBIAN	DSA-3195

Vulnerability Solution:

- Upgrade to PHP version 5.4.38
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.5.22
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.6.6
Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.60. PHP Vulnerability: CVE-2015-1351 (php-cve-2015-1351)

Description:

Use-after-free vulnerability in the `_zend_shared_memdup` function in `zend_shared_alloc.c` in the OPcache extension in PHP through 5.6.7 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2015-1351

Vulnerability Solution:

Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.61. PHP Vulnerability: CVE-2015-1353 (php-cve-2015-1353)*Description:*

Multiple integer overflows in the calendar extension in PHP through 5.6.7 allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted year value to (1) the `GregorianToSdn` function in `gregor.c` or (2) the `JulianToSdn` function in `julian.c`, as demonstrated by a crafted third argument to the `gregoriantojd` or `juliantojd` function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2015-1353

Vulnerability Solution:

Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.62. PHP Vulnerability: CVE-2015-2301 (php-cve-2015-2301)*Description:*

Use-after-free vulnerability in the `phar_rename_archive` function in `phar_object.c` in PHP before 5.5.22 and 5.6.x before 5.6.6 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted renaming of a Phar archive to the name of an existing file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2015-2301
DEBIAN	DSA-3198

Vulnerability Solution:

- Upgrade to PHP version 5.5.22
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.6.6
Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.63. PHP Vulnerability: CVE-2015-2331 (php-cve-2015-2331)

Description:

Integer overflow in the `_zip_cdir_new` function in `zip_dirent.c` in `libzip` 0.11.2 and earlier, as used in the ZIP extension in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a ZIP archive that contains many entries, leading to a heap-based buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2015-2331
DEBIAN	DSA-3198

Vulnerability Solution:

- Upgrade to PHP version 5.4.39
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.5.23
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.6.7
Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.64. PHP Vulnerability: CVE-2015-2787 (php-cve-2015-2787)

Description:

Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages use of the unset function within an __wakeup function, a related issue to CVE-2015-0231.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2015-2787

Vulnerability Solution:

- Upgrade to PHP version 5.4.39
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.5.23
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.6.7
Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.65. 'rlogin' Remote Login Service Enabled (service-rlogin)

Description:

The RSH remote login service (rlogin) is enabled. This is a legacy service often configured to blindly trust some hosts and IPs. The protocol also doesn't support encryption or any sort of strong authentication mechanism.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:513	Running Remote Login service

References:

Source	Reference
CVE	CVE-1999-0651

Vulnerability Solution:

Disable or firewall this service which usually runs on 513/tcp.

3.1.66. 'rsh' Remote Shell Service Enabled (service-rsh)*Description:*

The RSH remote shell service (rsh) is enabled. This is a legacy service often configured to blindly trust some hosts and IPs. The protocol also doesn't support encryption or any sort of strong authentication mechanism.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:514	Running Remote Shell service

References:

Source	Reference
CVE	CVE-1999-0651

Vulnerability Solution:

Disable or firewall this service which usually runs on 514/tcp.

3.1.67. USN-1082-1: Pango vulnerabilities (ubuntu-usn-1082-1)*Description:*

Heap-based buffer overflow in the pango_ft2_font_render_box_glyph function in pango/pangoft2-render.c in libpango in Pango 1.28.3 and earlier, when the FreeType2 backend is enabled, allows user-assisted remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file, related to the glyph box for an FT_Bitmap object.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04

Affected Nodes:	Additional Information:
	Vulnerable software installed: Ubuntu libpango1.0-0 1.20.5-0ubuntu1.1

References:

Source	Reference
BID	38760
BID	45842
BID	46632
CVE	CVE-2010-0421
CVE	CVE-2011-0020
CVE	CVE-2011-0064
DEBIAN	DSA-2019
DEBIAN	DSA-2178
OSVDB	70596
OVAL	OVAL9417
REDHAT	RHSA-2010:0140
REDHAT	RHSA-2011:0180
REDHAT	RHSA-2011:0309
USN	USN-1082-1
XF	64832
XF	65770

Vulnerability Solution:

- gir1.0-pango-1.0 on Ubuntu Linux 10.04
Upgrade gir1.0-pango-1.0 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade gir1.0-pango-1.0 to the latest version
- gir1.0-pango-1.0 on Ubuntu Linux 10.10
Upgrade gir1.0-pango-1.0 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade gir1.0-pango-1.0 to the latest version
- libpango1.0-0 on Ubuntu Linux 8.04
Upgrade libpango1.0-0 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libpango1.0-0 to the latest version
- libpango1.0-0 on Ubuntu Linux 9.10
Upgrade libpango1.0-0 for Ubuntu 9.10
Use `apt-get upgrade` to upgrade libpango1.0-0 to the latest version

3.1.68. USN-1108-1: DHCP vulnerability (ubuntu-usn-1108-1)*Description:*

dhclient in ISC DHCP 3.0.x through 4.2.x before 4.2.1-P1, 3.1-ESV before 3.1-ESV-R1, and 4.1-ESV before 4.1-ESV-R2 allows remote attackers to execute arbitrary commands via shell metacharacters in a hostname obtained from a DHCP message, as demonstrated by a hostname that is provided to dhclient-script.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu dhcp3-client 3.0.6.dfsg-1ubuntu9

References:

Source	Reference
BID	47176
CERT-VN	107886
CVE	CVE-2011-0997
DEBIAN	DSA-2216
DEBIAN	DSA-2217
DISA_SEVERITY	Category I
DISA_VMSKEY	V0029562
IAVM	2011-A-0108
OSVDB	71493
OVAL	OVAL12812
REDHAT	RHSA-2011:0428
REDHAT	RHSA-2011:0840
USN	USN-1108-1
XF	66580

Vulnerability Solution:

•dhcp3-client on Ubuntu Linux 10.04

Upgrade dhcp3-client for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade dhcp3-client to the latest version

•dhcp3-client on Ubuntu Linux 10.10

Upgrade dhcp3-client for Ubuntu 10.10

Use `apt-get upgrade` to upgrade dhcp3-client to the latest version

- dhcp3-client on Ubuntu Linux 8.04

Upgrade dhcp3-client for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade dhcp3-client to the latest version

- dhcp3-client on Ubuntu Linux 9.10

Upgrade dhcp3-client for Ubuntu 9.10

Use `apt-get upgrade` to upgrade dhcp3-client to the latest version

3.1.69. USN-1126-1: PHP vulnerabilities (ubuntu-usn-1126-1)

Description:

Multiple format string vulnerabilities in phar_object.c in the phar extension in PHP 5.3.5 and earlier allow context-dependent attackers to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code via format string specifiers in an argument to a class method, leading to an incorrect zend_throw_exception_ex call.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu php5-gd 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
APPLE	APPLE-SA-2011-10-12-3
APPLE	APPLE-SA-2012-02-01-1
BID	45338
BID	45952
BID	46354
BID	46365
BID	46429
BID	46605
BID	46786
BID	46843
BID	46854
BID	46928
BID	46967

Source	Reference
BID	46968
BID	46969
BID	46970
BID	46975
BID	46977
BID	49241
CERT-VN	210829
CVE	CVE-2006-7243
CVE	CVE-2010-4697
CVE	CVE-2010-4698
CVE	CVE-2011-0420
CVE	CVE-2011-0421
CVE	CVE-2011-0441
CVE	CVE-2011-0708
CVE	CVE-2011-1072
CVE	CVE-2011-1092
CVE	CVE-2011-1144
CVE	CVE-2011-1148
CVE	CVE-2011-1153
CVE	CVE-2011-1464
CVE	CVE-2011-1466
CVE	CVE-2011-1467
CVE	CVE-2011-1468
CVE	CVE-2011-1469
CVE	CVE-2011-1470
CVE	CVE-2011-1471
DEBIAN	DSA-2266
OVAL	OVAL11939
OVAL	OVAL12528
OVAL	OVAL12569
REDHAT	RHSA-2011:1423
REDHAT	RHSA-2011:1741
REDHAT	RHSA-2012:0071

Source	Reference
REDHAT	RHSA-2013:1307
REDHAT	RHSA-2013:1615
REDHAT	RHSA-2014:0311
USN	USN-1126-1
XF	65310
XF	65437
XF	65721
XF	65911
XF	65988
XF	66079
XF	66080
XF	66173
XF	66180

Vulnerability Solution:

- libapache2-mod-php5 on Ubuntu Linux 10.04
Upgrade libapache2-mod-php5 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- libapache2-mod-php5 on Ubuntu Linux 10.10
Upgrade libapache2-mod-php5 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- libapache2-mod-php5 on Ubuntu Linux 11.04
Upgrade libapache2-mod-php5 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- libapache2-mod-php5 on Ubuntu Linux 8.04
Upgrade libapache2-mod-php5 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- libapache2-mod-php5 on Ubuntu Linux 9.10
Upgrade libapache2-mod-php5 for Ubuntu 9.10
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- php-pear on Ubuntu Linux 10.04
Upgrade php-pear for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade php-pear to the latest version
- php-pear on Ubuntu Linux 10.10
Upgrade php-pear for Ubuntu 10.10
Use `apt-get upgrade` to upgrade php-pear to the latest version
- php-pear on Ubuntu Linux 11.04
Upgrade php-pear for Ubuntu 11.04

Use `apt-get upgrade` to upgrade php-pear to the latest version

- php-pear on Ubuntu Linux 8.04
Upgrade php-pear for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade php-pear to the latest version
- php-pear on Ubuntu Linux 9.10
Upgrade php-pear for Ubuntu 9.10
Use `apt-get upgrade` to upgrade php-pear to the latest version
- php5 on Ubuntu Linux 10.04
Upgrade php5 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade php5 to the latest version
- php5 on Ubuntu Linux 10.10
Upgrade php5 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade php5 to the latest version
- php5 on Ubuntu Linux 11.04
Upgrade php5 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade php5 to the latest version
- php5 on Ubuntu Linux 8.04
Upgrade php5 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade php5 to the latest version
- php5 on Ubuntu Linux 9.10
Upgrade php5 for Ubuntu 9.10
Use `apt-get upgrade` to upgrade php5 to the latest version
- php5-cgi on Ubuntu Linux 10.04
Upgrade php5-cgi for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 10.10
Upgrade php5-cgi for Ubuntu 10.10
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 11.04
Upgrade php5-cgi for Ubuntu 11.04
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 8.04
Upgrade php5-cgi for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 9.10
Upgrade php5-cgi for Ubuntu 9.10
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cli on Ubuntu Linux 10.04
Upgrade php5-cli for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade php5-cli to the latest version

- php5-cli on Ubuntu Linux 10.10
Upgrade php5-cli for Ubuntu 10.10
Use `apt-get upgrade` to upgrade php5-cli to the latest version
- php5-cli on Ubuntu Linux 11.04
Upgrade php5-cli for Ubuntu 11.04
Use `apt-get upgrade` to upgrade php5-cli to the latest version
- php5-cli on Ubuntu Linux 8.04
Upgrade php5-cli for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade php5-cli to the latest version
- php5-cli on Ubuntu Linux 9.10
Upgrade php5-cli for Ubuntu 9.10
Use `apt-get upgrade` to upgrade php5-cli to the latest version
- php5-common on Ubuntu Linux 10.04
Upgrade php5-common for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade php5-common to the latest version
- php5-common on Ubuntu Linux 10.10
Upgrade php5-common for Ubuntu 10.10
Use `apt-get upgrade` to upgrade php5-common to the latest version
- php5-common on Ubuntu Linux 11.04
Upgrade php5-common for Ubuntu 11.04
Use `apt-get upgrade` to upgrade php5-common to the latest version
- php5-common on Ubuntu Linux 8.04
Upgrade php5-common for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade php5-common to the latest version
- php5-common on Ubuntu Linux 9.10
Upgrade php5-common for Ubuntu 9.10
Use `apt-get upgrade` to upgrade php5-common to the latest version
- php5-curl on Ubuntu Linux 10.04
Upgrade php5-curl for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade php5-curl to the latest version
- php5-curl on Ubuntu Linux 10.10
Upgrade php5-curl for Ubuntu 10.10
Use `apt-get upgrade` to upgrade php5-curl to the latest version
- php5-curl on Ubuntu Linux 11.04
Upgrade php5-curl for Ubuntu 11.04
Use `apt-get upgrade` to upgrade php5-curl to the latest version
- php5-curl on Ubuntu Linux 8.04
Upgrade php5-curl for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade php5-curl to the latest version
- php5-curl on Ubuntu Linux 9.10
Upgrade php5-curl for Ubuntu 9.10

Use `apt-get upgrade` to upgrade php5-curl to the latest version

- php5-dev on Ubuntu Linux 10.04

Upgrade php5-dev for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade php5-dev to the latest version

- php5-dev on Ubuntu Linux 10.10

Upgrade php5-dev for Ubuntu 10.10

Use `apt-get upgrade` to upgrade php5-dev to the latest version

- php5-dev on Ubuntu Linux 11.04

Upgrade php5-dev for Ubuntu 11.04

Use `apt-get upgrade` to upgrade php5-dev to the latest version

- php5-dev on Ubuntu Linux 8.04

Upgrade php5-dev for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade php5-dev to the latest version

- php5-dev on Ubuntu Linux 9.10

Upgrade php5-dev for Ubuntu 9.10

Use `apt-get upgrade` to upgrade php5-dev to the latest version

- php5-gd on Ubuntu Linux 10.04

Upgrade php5-gd for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade php5-gd to the latest version

- php5-gd on Ubuntu Linux 10.10

Upgrade php5-gd for Ubuntu 10.10

Use `apt-get upgrade` to upgrade php5-gd to the latest version

- php5-gd on Ubuntu Linux 11.04

Upgrade php5-gd for Ubuntu 11.04

Use `apt-get upgrade` to upgrade php5-gd to the latest version

- php5-gd on Ubuntu Linux 8.04

Upgrade php5-gd for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade php5-gd to the latest version

- php5-gd on Ubuntu Linux 9.10

Upgrade php5-gd for Ubuntu 9.10

Use `apt-get upgrade` to upgrade php5-gd to the latest version

- php5-intl on Ubuntu Linux 10.04

Upgrade php5-intl for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade php5-intl to the latest version

- php5-intl on Ubuntu Linux 10.10

Upgrade php5-intl for Ubuntu 10.10

Use `apt-get upgrade` to upgrade php5-intl to the latest version

- php5-intl on Ubuntu Linux 11.04

Upgrade php5-intl for Ubuntu 11.04

Use `apt-get upgrade` to upgrade php5-intl to the latest version

3.1.70. USN-1158-1: curl vulnerabilities (ubuntu-usn-1158-1)*Description:*

lib/ssluse.c in cURL and libcurl 7.4 through 7.19.5, when OpenSSL is used, does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libcurl3-gnutls 7.18.0-1ubuntu2

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
APPLE	APPLE-SA-2010-06-15-1
APPLE	APPLE-SA-2012-02-01-1
BID	36032
CVE	CVE-2009-2417
CVE	CVE-2010-0734
CVE	CVE-2011-2192
DEBIAN	DSA-2023
DEBIAN	DSA-2271
DISA_SEVERITY	Category I
DISA_VMSKEY	V0027158
DISA_VMSKEY	V0031252
IAVM	2011-A-0066
IAVM	2012-A-0020
OVAL	OVAL10114
OVAL	OVAL10760
OVAL	OVAL6756
OVAL	OVAL8542
REDHAT	RHSA-2010:0329
REDHAT	RHSA-2011:0918

Source	Reference
USN	USN-1158-1
XF	52405

Vulnerability Solution:

•libcurl3 on Ubuntu Linux 10.04

Upgrade libcurl3 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libcurl3 to the latest version

•libcurl3 on Ubuntu Linux 10.10

Upgrade libcurl3 for Ubuntu 10.10

Use `apt-get upgrade` to upgrade libcurl3 to the latest version

•libcurl3 on Ubuntu Linux 11.04

Upgrade libcurl3 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libcurl3 to the latest version

•libcurl3 on Ubuntu Linux 8.04

Upgrade libcurl3 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libcurl3 to the latest version

•libcurl3-gnutls on Ubuntu Linux 10.04

Upgrade libcurl3-gnutls for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libcurl3-gnutls to the latest version

•libcurl3-gnutls on Ubuntu Linux 10.10

Upgrade libcurl3-gnutls for Ubuntu 10.10

Use `apt-get upgrade` to upgrade libcurl3-gnutls to the latest version

•libcurl3-gnutls on Ubuntu Linux 11.04

Upgrade libcurl3-gnutls for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libcurl3-gnutls to the latest version

•libcurl3-gnutls on Ubuntu Linux 8.04

Upgrade libcurl3-gnutls for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libcurl3-gnutls to the latest version

•libcurl3-nss on Ubuntu Linux 11.04

Upgrade libcurl3-nss for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libcurl3-nss to the latest version

3.1.71. USN-1199-1: Apache vulnerability (ubuntu-usn-1199-1)*Description:*

The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu apache2-mpm-prefork 2.2.8-1ubuntu0.15

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	49303
CERT-VN	405811
CVE	CVE-2011-3192
OSVDB	74721
OVAL	OVAL14762
OVAL	OVAL14824
OVAL	OVAL18827
REDHAT	RHSA-2011:1245
REDHAT	RHSA-2011:1294
REDHAT	RHSA-2011:1300
REDHAT	RHSA-2011:1329
REDHAT	RHSA-2011:1330
REDHAT	RHSA-2011:1369
USN	USN-1199-1
XF	69396

Vulnerability Solution:

- apache2-mpm-event on Ubuntu Linux 8.04
Upgrade apache2-mpm-event for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade apache2-mpm-event to the latest version
- apache2-mpm-perchild on Ubuntu Linux 8.04
Upgrade apache2-mpm-perchild for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade apache2-mpm-perchild to the latest version
- apache2-mpm-prefork on Ubuntu Linux 8.04
Upgrade apache2-mpm-prefork for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade apache2-mpm-prefork to the latest version
- apache2-mpm-worker on Ubuntu Linux 8.04
Upgrade apache2-mpm-worker for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade apache2-mpm-worker to the latest version

- apache2.2-bin on Ubuntu Linux 10.04
Upgrade apache2.2-bin for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade apache2.2-bin to the latest version
- apache2.2-bin on Ubuntu Linux 10.10
Upgrade apache2.2-bin for Ubuntu 10.10
Use `apt-get upgrade` to upgrade apache2.2-bin to the latest version
- apache2.2-bin on Ubuntu Linux 11.04
Upgrade apache2.2-bin for Ubuntu 11.04
Use `apt-get upgrade` to upgrade apache2.2-bin to the latest version

3.1.72. USN-1231-1: PHP Vulnerabilities (ubuntu-usn-1231-1)

Description:

Stack-based buffer overflow in the socket_connect function in ext/sockets/sockets.c in PHP 5.3.3 through 5.3.6 might allow context-dependent attackers to execute arbitrary code via a long pathname for a UNIX socket.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu php5-common 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2010-08-24-1
APPLE	APPLE-SA-2010-11-10-1
APPLE	APPLE-SA-2012-02-01-1
BID	48259
BID	49241
BID	49249
BID	49252
CVE	CVE-2010-1914
CVE	CVE-2010-2484
CVE	CVE-2011-1657
CVE	CVE-2011-1938
CVE	CVE-2011-2202

Source	Reference
CVE	CVE-2011-2483
CVE	CVE-2011-3182
CVE	CVE-2011-3267
DEBIAN	DSA-2266
DEBIAN	DSA-2340
DEBIAN	DSA-2399
OSVDB	72644
OSVDB	74739
REDHAT	RHSA-2011:1377
REDHAT	RHSA-2011:1378
REDHAT	RHSA-2011:1423
REDHAT	RHSA-2012:0071
SUSE	SUSE-SA:2011:035
USN	USN-1231-1
XF	58587
XF	67606
XF	67999
XF	69319
XF	69320
XF	69428
XF	69430

Vulnerability Solution:

- libapache2-mod-php5 on Ubuntu Linux 10.04
Upgrade libapache2-mod-php5 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- libapache2-mod-php5 on Ubuntu Linux 10.10
Upgrade libapache2-mod-php5 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- libapache2-mod-php5 on Ubuntu Linux 11.04
Upgrade libapache2-mod-php5 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- libapache2-mod-php5 on Ubuntu Linux 11.10
Upgrade libapache2-mod-php5 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version

- libapache2-mod-php5 on Ubuntu Linux 8.04

Upgrade libapache2-mod-php5 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version

- php5-cgi on Ubuntu Linux 10.04

Upgrade php5-cgi for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade php5-cgi to the latest version

- php5-cgi on Ubuntu Linux 10.10

Upgrade php5-cgi for Ubuntu 10.10

Use `apt-get upgrade` to upgrade php5-cgi to the latest version

- php5-cgi on Ubuntu Linux 11.04

Upgrade php5-cgi for Ubuntu 11.04

Use `apt-get upgrade` to upgrade php5-cgi to the latest version

- php5-cgi on Ubuntu Linux 11.10

Upgrade php5-cgi for Ubuntu 11.10

Use `apt-get upgrade` to upgrade php5-cgi to the latest version

- php5-cgi on Ubuntu Linux 8.04

Upgrade php5-cgi for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade php5-cgi to the latest version

- php5-cli on Ubuntu Linux 10.04

Upgrade php5-cli for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade php5-cli to the latest version

- php5-cli on Ubuntu Linux 10.10

Upgrade php5-cli for Ubuntu 10.10

Use `apt-get upgrade` to upgrade php5-cli to the latest version

- php5-cli on Ubuntu Linux 11.04

Upgrade php5-cli for Ubuntu 11.04

Use `apt-get upgrade` to upgrade php5-cli to the latest version

- php5-cli on Ubuntu Linux 11.10

Upgrade php5-cli for Ubuntu 11.10

Use `apt-get upgrade` to upgrade php5-cli to the latest version

- php5-cli on Ubuntu Linux 8.04

Upgrade php5-cli for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade php5-cli to the latest version

- php5-common on Ubuntu Linux 10.04

Upgrade php5-common for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade php5-common to the latest version

- php5-common on Ubuntu Linux 10.10

Upgrade php5-common for Ubuntu 10.10

Use `apt-get upgrade` to upgrade php5-common to the latest version

- php5-common on Ubuntu Linux 11.04

Upgrade php5-common for Ubuntu 11.04

Use `apt-get upgrade` to upgrade php5-common to the latest version

- php5-common on Ubuntu Linux 11.10

Upgrade php5-common for Ubuntu 11.10

Use `apt-get upgrade` to upgrade php5-common to the latest version

- php5-common on Ubuntu Linux 8.04

Upgrade php5-common for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade php5-common to the latest version

3.1.73. USN-1358-1: PHP vulnerabilities (ubuntu-usn-1358-1)

Description:

The php_register_variable_ex function in php_variables.c in PHP 5.3.9 allows remote attackers to execute arbitrary code via a request containing a large number of variables, related to improper handling of array variables. NOTE: this vulnerability exists because of an incorrect fix for CVE-2011-4885.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu php5-common 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2012-05-09-1
APPLE	APPLE-SA-2012-09-19-2
BID	46928
BID	51193
BID	51830
BID	51954
CERT-VN	903934
CVE	CVE-2011-0441
CVE	CVE-2011-4153
CVE	CVE-2011-4885
CVE	CVE-2012-0057
CVE	CVE-2012-0788
CVE	CVE-2012-0830

Source	Reference
CVE	CVE-2012-0831
DEBIAN	DSA-2399
DEBIAN	DSA-2403
OSVDB	78819
REDHAT	RHSA-2012:0019
REDHAT	RHSA-2012:0071
REDHAT	RHSA-2012:0092
REDHAT	RHSA-2013:1307
USN	USN-1358-1
XF	66180
XF	72021
XF	72908
XF	72911
XF	73125

Vulnerability Solution:

- libapache2-mod-php5 on Ubuntu Linux 10.04
Upgrade libapache2-mod-php5 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- libapache2-mod-php5 on Ubuntu Linux 10.10
Upgrade libapache2-mod-php5 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- libapache2-mod-php5 on Ubuntu Linux 11.04
Upgrade libapache2-mod-php5 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- libapache2-mod-php5 on Ubuntu Linux 11.10
Upgrade libapache2-mod-php5 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- libapache2-mod-php5 on Ubuntu Linux 8.04
Upgrade libapache2-mod-php5 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- php5 on Ubuntu Linux 10.04
Upgrade php5 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade php5 to the latest version
- php5 on Ubuntu Linux 10.10
Upgrade php5 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade php5 to the latest version

- php5 on Ubuntu Linux 11.04
Upgrade php5 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade php5 to the latest version
- php5 on Ubuntu Linux 11.10
Upgrade php5 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade php5 to the latest version
- php5 on Ubuntu Linux 8.04
Upgrade php5 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade php5 to the latest version
- php5-cgi on Ubuntu Linux 10.04
Upgrade php5-cgi for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 10.10
Upgrade php5-cgi for Ubuntu 10.10
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 11.04
Upgrade php5-cgi for Ubuntu 11.04
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 11.10
Upgrade php5-cgi for Ubuntu 11.10
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 8.04
Upgrade php5-cgi for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cli on Ubuntu Linux 10.04
Upgrade php5-cli for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade php5-cli to the latest version
- php5-cli on Ubuntu Linux 10.10
Upgrade php5-cli for Ubuntu 10.10
Use `apt-get upgrade` to upgrade php5-cli to the latest version
- php5-cli on Ubuntu Linux 11.04
Upgrade php5-cli for Ubuntu 11.04
Use `apt-get upgrade` to upgrade php5-cli to the latest version
- php5-cli on Ubuntu Linux 11.10
Upgrade php5-cli for Ubuntu 11.10
Use `apt-get upgrade` to upgrade php5-cli to the latest version
- php5-cli on Ubuntu Linux 8.04
Upgrade php5-cli for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade php5-cli to the latest version
- php5-common on Ubuntu Linux 10.04
Upgrade php5-common for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade php5-common to the latest version

- php5-common on Ubuntu Linux 10.10
Upgrade php5-common for Ubuntu 10.10
Use `apt-get upgrade` to upgrade php5-common to the latest version
- php5-common on Ubuntu Linux 11.04
Upgrade php5-common for Ubuntu 11.04
Use `apt-get upgrade` to upgrade php5-common to the latest version
- php5-common on Ubuntu Linux 11.10
Upgrade php5-common for Ubuntu 11.10
Use `apt-get upgrade` to upgrade php5-common to the latest version
- php5-common on Ubuntu Linux 8.04
Upgrade php5-common for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade php5-common to the latest version
- php5-xsl on Ubuntu Linux 10.04
Upgrade php5-xsl for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade php5-xsl to the latest version
- php5-xsl on Ubuntu Linux 10.10
Upgrade php5-xsl for Ubuntu 10.10
Use `apt-get upgrade` to upgrade php5-xsl to the latest version
- php5-xsl on Ubuntu Linux 11.04
Upgrade php5-xsl for Ubuntu 11.04
Use `apt-get upgrade` to upgrade php5-xsl to the latest version
- php5-xsl on Ubuntu Linux 11.10
Upgrade php5-xsl for Ubuntu 11.10
Use `apt-get upgrade` to upgrade php5-xsl to the latest version
- php5-xsl on Ubuntu Linux 8.04
Upgrade php5-xsl for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade php5-xsl to the latest version

3.1.74. USN-1367-1: libpng vulnerabilities (ubuntu-usn-1367-1)

Description:

Integer overflow in libpng, as used in Google Chrome before 17.0.963.56, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an integer truncation.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04

Affected Nodes:	Additional Information:
	Vulnerable software installed: Ubuntu libpng12-0 1.2.15~beta5-3ubuntu0.2

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-1
APPLE	APPLE-SA-2012-09-19-2
CVE	CVE-2009-5063
CVE	CVE-2011-3026
OVAL	OVAL15032
USN	USN-1367-1

Vulnerability Solution:

- libpng12-0 on Ubuntu Linux 10.04
Upgrade libpng12-0 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 10.10
Upgrade libpng12-0 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 11.04
Upgrade libpng12-0 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 11.10
Upgrade libpng12-0 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 8.04
Upgrade libpng12-0 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version

3.1.75. USN-1374-1: Samba vulnerability (ubuntu-usn-1374-1)*Description:*

Heap-based buffer overflow in process.c in smbd in Samba 3.0, as used in the file-sharing service on the BlackBerry PlayBook tablet before 2.0.0.7971 and other products, allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code via a Batched (aka AndX) request that triggers infinite recursion.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu samba 3.0.20-0.1ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2012-05-09-1
CVE	CVE-2012-0870
USN	USN-1374-1
XF	73361

Vulnerability Solution:

samba on Ubuntu Linux 8.04

Use `apt-get upgrade` to upgrade samba to the latest version

3.1.76. USN-1396-1: GNU C Library vulnerabilities (ubuntu-usn-1396-1)*Description:*

nis/nss_nis/nis-pwd.c in the GNU C Library (aka glibc or libc6) 2.7 and Embedded GLIBC (EGLIBC) 2.10.2 adds information from the passwd.adjunct.byname map to entries in the passwd map, which allows remote attackers to obtain the encrypted passwords of NIS accounts by calling the getpwnam function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libc6 2.7-10ubuntu5

References:

Source	Reference
BID	46563
BID	46740
BID	52201
CVE	CVE-2009-5029
CVE	CVE-2010-0015
CVE	CVE-2011-1071
CVE	CVE-2011-1089

Source	Reference
CVE	CVE-2011-1095
CVE	CVE-2011-1658
CVE	CVE-2011-1659
CVE	CVE-2011-2702
CVE	CVE-2011-4609
CVE	CVE-2012-0864
DISA_SEVERITY	Category I
DISA_VMSKEY	V0029562
DISA_VMSKEY	V0030545
DISA_VMSKEY	V0033794
DISA_VMSKEY	V0033884
IAVM	2011-A-0108
IAVM	2011-A-0147
IAVM	2012-A-0148
IAVM	2012-A-0153
OSVDB	80718
OVAL	OVAL12272
OVAL	OVAL12853
REDHAT	RHSA-2011:0412
REDHAT	RHSA-2011:0413
REDHAT	RHSA-2011:1526
REDHAT	RHSA-2012:0393
REDHAT	RHSA-2012:0397
REDHAT	RHSA-2012:0488
REDHAT	RHSA-2012:0531
USN	USN-1396-1
XF	66819
XF	66820

Vulnerability Solution:

- libc-bin on Ubuntu Linux 10.04

Upgrade libc-bin for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libc-bin to the latest version

- libc-bin on Ubuntu Linux 10.10

Upgrade libc-bin for Ubuntu 10.10

Use `apt-get upgrade` to upgrade libc-bin to the latest version

- libc6 on Ubuntu Linux 10.04

Upgrade libc6 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libc6 to the latest version

- libc6 on Ubuntu Linux 10.10

Upgrade libc6 for Ubuntu 10.10

Use `apt-get upgrade` to upgrade libc6 to the latest version

- libc6 on Ubuntu Linux 11.04

Upgrade libc6 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libc6 to the latest version

- libc6 on Ubuntu Linux 11.10

Upgrade libc6 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libc6 to the latest version

- libc6 on Ubuntu Linux 8.04

Upgrade libc6 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libc6 to the latest version

3.1.77. USN-1437-1: PHP vulnerability (ubuntu-usn-1437-1)

Description:

sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu php5-cgi 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
CERT-VN	520827
CERT-VN	673343
CVE	CVE-2012-1823
CVE	CVE-2012-2311

Source	Reference
REDHAT	RHSA-2012:0546
REDHAT	RHSA-2012:0547
REDHAT	RHSA-2012:0568
USN	USN-1437-1

Vulnerability Solution:

- php5-cgi on Ubuntu Linux 10.04
Upgrade php5-cgi for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 11.04
Upgrade php5-cgi for Ubuntu 11.04
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 11.10
Upgrade php5-cgi for Ubuntu 11.10
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 12.04
Upgrade php5-cgi for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 8.04
Upgrade php5-cgi for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade php5-cgi to the latest version

3.1.78. USN-1498-1: tiff vulnerabilities (ubuntu-usn-1498-1)*Description:*

Integer signedness error in the TIFFReadDirectory function in tif_dirread.c in libtiff 3.9.4 and earlier allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a negative tile depth in a tiff image, which triggers an improper conversion between signed and unsigned types, leading to a heap-based buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libtiff4 3.8.2-7ubuntu3.4

References:

Source	Reference
APPLE	APPLE-SA-2013-03-14-1

Source	Reference
BID	54076
BID	54270
CVE	CVE-2012-2088
CVE	CVE-2012-2113
DEBIAN	DSA-2552
DISA_SEVERITY	Category I
DISA_VMSKEY	V0036903
IAVM	2013-A-0048
REDHAT	RHSA-2012:1054
USN	USN-1498-1

Vulnerability Solution:

- libtiff-tools on Ubuntu Linux 10.04

Upgrade libtiff-tools for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libtiff-tools to the latest version

- libtiff-tools on Ubuntu Linux 11.04

Upgrade libtiff-tools for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libtiff-tools to the latest version

- libtiff-tools on Ubuntu Linux 11.10

Upgrade libtiff-tools for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libtiff-tools to the latest version

- libtiff-tools on Ubuntu Linux 12.04

Upgrade libtiff-tools for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libtiff-tools to the latest version

- libtiff-tools on Ubuntu Linux 8.04

Upgrade libtiff-tools for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libtiff-tools to the latest version

- libtiff4 on Ubuntu Linux 10.04

Upgrade libtiff4 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

- libtiff4 on Ubuntu Linux 11.04

Upgrade libtiff4 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

- libtiff4 on Ubuntu Linux 11.10

Upgrade libtiff4 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

- libtiff4 on Ubuntu Linux 12.04

Upgrade libtiff4 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

- libtiff4 on Ubuntu Linux 8.04

Upgrade libtiff4 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

3.1.79. USN-1601-1: Bind vulnerability (ubuntu-usn-1601-1)

Description:

ISC BIND 9.x before 9.7.6-P4, 9.8.x before 9.8.3-P4, 9.9.x before 9.9.1-P4, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P4 allows remote attackers to cause a denial of service (named daemon hang) via unspecified combinations of resource records.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu bind9 1:9.4.2-10

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
BID	55852
CVE	CVE-2012-5166
DEBIAN	DSA-2560
OSVDB	86118
OVAL	OVAL19706
REDHAT	RHSA-2012:1363
REDHAT	RHSA-2012:1364
REDHAT	RHSA-2012:1365
USN	USN-1601-1

Vulnerability Solution:

- bind9 on Ubuntu Linux 10.04

Upgrade bind9 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade bind9 to the latest version

- bind9 on Ubuntu Linux 11.04

Upgrade bind9 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade bind9 to the latest version

- bind9 on Ubuntu Linux 11.10

Upgrade bind9 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade bind9 to the latest version

- bind9 on Ubuntu Linux 12.04

Upgrade bind9 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade bind9 to the latest version

- bind9 on Ubuntu Linux 8.04

Upgrade bind9 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade bind9 to the latest version

3.1.80. USN-1643-1: Perl vulnerabilities (ubuntu-usn-1643-1)

Description:

Heap-based buffer overflow in the Perl_repeatcpy function in util.c in Perl 5.12.x before 5.12.5, 5.14.x before 5.14.3, and 5.15.x before 5.15.5 allows context-dependent attackers to cause a denial of service (memory consumption and crash) or possibly execute arbitrary code via the 'x' string repeat operator.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu perl 5.8.8-12ubuntu0.5

References:

Source	Reference
BID	49858
BID	49911
BID	56287
BID	56562
CVE	CVE-2011-2939
CVE	CVE-2011-3597
CVE	CVE-2012-5195
CVE	CVE-2012-5526
DEBIAN	DSA-2586
DISA_SEVERITY	Category I
DISA_VMSKEY	V0033794
DISA_VMSKEY	V0033884
IAVM	2012-A-0148

Source	Reference
IAVM	2012-A-0153
OVAL	OVAL19446
REDHAT	RHSA-2011:1424
REDHAT	RHSA-2011:1797
REDHAT	RHSA-2013:0685
USN	USN-1643-1
XF	80098

Vulnerability Solution:

- perl on Ubuntu Linux 10.04
Upgrade perl for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade perl to the latest version
- perl on Ubuntu Linux 11.10
Upgrade perl for Ubuntu 11.10
Use `apt-get upgrade` to upgrade perl to the latest version
- perl on Ubuntu Linux 12.04
Upgrade perl for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade perl to the latest version
- perl on Ubuntu Linux 12.10
Upgrade perl for Ubuntu 12.10
Use `apt-get upgrade` to upgrade perl to the latest version
- perl on Ubuntu Linux 8.04
Upgrade perl for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade perl to the latest version

3.1.81. USN-1770-1: Perl vulnerability (ubuntu-usn-1770-1)*Description:*

The rehash mechanism in Perl 5.8.2 through 5.16.x allows context-dependent attackers to cause a denial of service (memory consumption and crash) via a crafted hash key.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu perl 5.8.8-12ubuntu0.5

References:

Source	Reference
APPLE	APPLE-SA-2013-10-22-3
BID	58311
CVE	CVE-2013-1667
DEBIAN	DSA-2641
OSVDB	90892
OVAL	OVAL18771
REDHAT	RHSA-2013:0685
USN	USN-1770-1
XF	82598

Vulnerability Solution:

- perl on Ubuntu Linux 10.04
Upgrade perl for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade perl to the latest version
- perl on Ubuntu Linux 11.10
Upgrade perl for Ubuntu 11.10
Use `apt-get upgrade` to upgrade perl to the latest version
- perl on Ubuntu Linux 12.04
Upgrade perl for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade perl to the latest version
- perl on Ubuntu Linux 12.10
Upgrade perl for Ubuntu 12.10
Use `apt-get upgrade` to upgrade perl to the latest version
- perl on Ubuntu Linux 8.04
Upgrade perl for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade perl to the latest version

3.1.82. USN-612-2: OpenSSH vulnerability (ubuntu-usn-612-2)*Description:*

OpenSSL 0.9.8c-1 up to versions before 0.9.8g-9 on Debian-based operating systems uses a random number generator that generates predictable numbers, which makes it easier for remote attackers to conduct brute force guessing attacks against cryptographic keys.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04

Affected Nodes:	Additional Information:
	Vulnerable software installed: Ubuntu openssh-server 1:4.7p1-8ubuntu1

References:

Source	Reference
BID	29179
CERT	TA08-137A
CERT-VN	925211
CVE	CVE-2008-0166
DEBIAN	DSA-1571
DEBIAN	DSA-1576
USN	USN-612-2
XF	42375

Vulnerability Solution:

- openssh-client on Ubuntu Linux 7.04
Upgrade openssh-client for Ubuntu 7.04
Use `apt-get upgrade` to upgrade openssh-client to the latest version
- openssh-client on Ubuntu Linux 7.10
Upgrade openssh-client for Ubuntu 7.10
Use `apt-get upgrade` to upgrade openssh-client to the latest version
- openssh-client on Ubuntu Linux 8.04
Upgrade openssh-client for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade openssh-client to the latest version
- openssh-server on Ubuntu Linux 7.04
Upgrade openssh-server for Ubuntu 7.04
Use `apt-get upgrade` to upgrade openssh-server to the latest version
- openssh-server on Ubuntu Linux 7.10
Upgrade openssh-server for Ubuntu 7.10
Use `apt-get upgrade` to upgrade openssh-server to the latest version
- openssh-server on Ubuntu Linux 8.04
Upgrade openssh-server for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade openssh-server to the latest version

3.1.83. USN-612-4: ssl-cert vulnerability (ubuntu-usn-612-4)*Description:*

OpenSSL 0.9.8c-1 up to versions before 0.9.8g-9 on Debian-based operating systems uses a random number generator that generates predictable numbers, which makes it easier for remote attackers to conduct brute force guessing attacks against cryptographic keys.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu ssl-cert 1.0.14-0ubuntu2

References:

Source	Reference
BID	29179
CERT	TA08-137A
CERT-VN	925211
CVE	CVE-2008-0166
DEBIAN	DSA-1571
DEBIAN	DSA-1576
USN	USN-612-4
XF	42375

Vulnerability Solution:

- ssl-cert on Ubuntu Linux 7.04
Upgrade ssl-cert for Ubuntu 7.04
Use `apt-get upgrade` to upgrade ssl-cert to the latest version
- ssl-cert on Ubuntu Linux 7.10
Upgrade ssl-cert for Ubuntu 7.10
Use `apt-get upgrade` to upgrade ssl-cert to the latest version
- ssl-cert on Ubuntu Linux 8.04
Upgrade ssl-cert for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade ssl-cert to the latest version

3.1.84. USN-624-1: PCRE vulnerability (ubuntu-usn-624-1)*Description:*

Heap-based buffer overflow in pcre_compile.c in the Perl-Compatible Regular Expression (PCRE) library 7.7 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a regular expression that begins with an option and contains multiple branches.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libpcre3 7.4-1ubuntu2

References:

Source	Reference
APPLE	APPLE-SA-2008-10-09
APPLE	APPLE-SA-2009-05-12
BID	30087
BID	31681
CERT	TA09-133A
CVE	CVE-2008-2371
DEBIAN	DSA-1602
USN	USN-624-1

Vulnerability Solution:

- libpcre3 on Ubuntu Linux 7.04
Upgrade libpcre3 for Ubuntu 7.04
Use `apt-get upgrade` to upgrade libpcre3 to the latest version
- libpcre3 on Ubuntu Linux 7.10
Upgrade libpcre3 for Ubuntu 7.10
Use `apt-get upgrade` to upgrade libpcre3 to the latest version
- libpcre3 on Ubuntu Linux 8.04
Upgrade libpcre3 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libpcre3 to the latest version

3.1.85. USN-786-1: apr-util vulnerabilities (ubuntu-usn-786-1)*Description:*

The expat XML parser in the apr_xml_* interface in xml/apr_xml.c in Apache APR-util before 1.3.7, as used in the mod_dav and mod_dav_svn modules in the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via a crafted XML document containing a large number of nested entity references, as demonstrated by a PROPFIND request, a similar issue to CVE-2003-1564.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libaprutil1 1.2.12+dfsg-3

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
BID	35221
BID	35251
BID	35253
CVE	CVE-2009-0023
CVE	CVE-2009-1955
CVE	CVE-2009-1956
DEBIAN	DSA-1812
OVAL	OVAL10270
OVAL	OVAL10968
OVAL	OVAL11567
OVAL	OVAL12237
OVAL	OVAL12321
OVAL	OVAL12473
REDHAT	RHSA-2009:1107
REDHAT	RHSA-2009:1108
USN	USN-786-1
XF	50964

Vulnerability Solution:

- libaprutil1 on Ubuntu Linux 8.04
Upgrade libaprutil1 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libaprutil1 to the latest version
- libaprutil1 on Ubuntu Linux 8.10
Upgrade libaprutil1 for Ubuntu 8.10
Use `apt-get upgrade` to upgrade libaprutil1 to the latest version
- libaprutil1 on Ubuntu Linux 9.04
Upgrade libaprutil1 for Ubuntu 9.04
Use `apt-get upgrade` to upgrade libaprutil1 to the latest version

3.1.86. USN-790-1: Cyrus SASL vulnerability (ubuntu-usn-790-1)

Description:

Multiple buffer overflows in the CMU Cyrus SASL library before 2.1.23 might allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via strings that are used as input to the sasl_encode64 function in lib/saslutil.c.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libsasl2-2 2.1.22.dfsg1-18ubuntu2

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
BID	34961
CERT	TA10-103B
CERT-VN	238019
CVE	CVE-2009-0688
DEBIAN	DSA-1807
OSVDB	54514
OSVDB	54515
OVAL	OVAL10687
OVAL	OVAL6136
REDHAT	RHSA-2009:1116
USN	USN-790-1
XF	50554

Vulnerability Solution:

- libsasl2-2 on Ubuntu Linux 8.04
Upgrade libsasl2-2 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libsasl2-2 to the latest version
- libsasl2-2 on Ubuntu Linux 8.10
Upgrade libsasl2-2 for Ubuntu 8.10
Use `apt-get upgrade` to upgrade libsasl2-2 to the latest version
- libsasl2-2 on Ubuntu Linux 9.04
Upgrade libsasl2-2 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade libsasl2-2 to the latest version

3.1.87. USN-809-1: GnuTLS vulnerabilities (ubuntu-usn-809-1)

Description:

libgnutls in GnuTLS before 2.8.2 does not properly handle a '\0' character in a domain name in the subject's (1) Common Name (CN) or (2) Subject Alternative Name (SAN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libgnutls13 2.0.4-1ubuntu2

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
CVE	CVE-2009-2409
CVE	CVE-2009-2730
DEBIAN	DSA-1874
DEBIAN	DSA-1888
OVAL	OVAL10763
OVAL	OVAL10778
OVAL	OVAL6631
OVAL	OVAL7155
OVAL	OVAL8409
OVAL	OVAL8594
REDHAT	RHSA-2009:1207
REDHAT	RHSA-2009:1232
REDHAT	RHSA-2009:1432
REDHAT	RHSA-2010:0095
USN	USN-809-1
XF	52404

Vulnerability Solution:

- libgnutls13 on Ubuntu Linux 8.04

Upgrade libgnutls13 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libgnutls13 to the latest version

- libgnutls26 on Ubuntu Linux 8.10

Upgrade libgnutls26 for Ubuntu 8.10

Use `apt-get upgrade` to upgrade libgnutls26 to the latest version

- libgnutls26 on Ubuntu Linux 9.04

Upgrade libgnutls26 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade libgnutls26 to the latest version

3.1.88. USN-944-1: GNU C Library vulnerabilities (ubuntu-usn-944-1)

Description:

Multiple integer overflows in libc in NetBSD 4.x, FreeBSD 6.x and 7.x, and probably other BSD and Apple Mac OS platforms allow context-dependent attackers to execute arbitrary code via large values of certain integer fields in the format argument to (1) the strfmon function in lib/libc/stdlib/strfmon.c, related to the GET_NUMBER macro; and (2) the printf function, related to left_prec and right_prec.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libc6 2.7-10ubuntu5

References:

Source	Reference
APPLE	APPLE-SA-2008-12-15
BID	28479
BID	40063
CERT	TA08-350A
CVE	CVE-2008-1391
CVE	CVE-2010-0296
CVE	CVE-2010-0830
DEBIAN	DSA-2058
DISA_SEVERITY	Category I
DISA_VMSKEY	V0030545
DISA_VMSKEY	V0033794
DISA_VMSKEY	V0033884

Source	Reference
IAVM	2011-A-0147
IAVM	2012-A-0148
IAVM	2012-A-0153
REDHAT	RHSA-2011:0412
USN	USN-944-1
XF	41504
XF	58915
XF	59240

Vulnerability Solution:

•libc6 on Ubuntu Linux 10.04

Upgrade libc6 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libc6 to the latest version

•libc6 on Ubuntu Linux 8.04

Upgrade libc6 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libc6 to the latest version

•libc6 on Ubuntu Linux 9.04

Upgrade libc6 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade libc6 to the latest version

•libc6 on Ubuntu Linux 9.10

Upgrade libc6 for Ubuntu 9.10

Use `apt-get upgrade` to upgrade libc6 to the latest version

3.1.89. USN-951-1: Samba vulnerability (ubuntu-usn-951-1)*Description:*

Buffer overflow in the SMB1 packet chaining implementation in the chain_reply function in process.c in smbd in Samba 3.0.x before 3.3.13 allows remote attackers to cause a denial of service (memory corruption and daemon crash) or possibly execute arbitrary code via a crafted field in a packet.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu samba 3.0.20-0.1ubuntu1

References:

--	--

Source	Reference
APPLE	APPLE-SA-2010-08-24-1
BID	40884
CVE	CVE-2010-2063
DEBIAN	DSA-2061
OSVDB	65518
OVAL	OVAL12427
OVAL	OVAL7115
OVAL	OVAL9859
REDHAT	RHSA-2010:0488
USN	USN-951-1
XF	59481

Vulnerability Solution:

•samba on Ubuntu Linux 8.04

Upgrade samba for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade samba to the latest version

•samba on Ubuntu Linux 9.04

Upgrade samba for Ubuntu 9.04

Use `apt-get upgrade` to upgrade samba to the latest version

3.1.90. USN-960-1: libpng vulnerabilities (ubuntu-usn-960-1)*Description:*

Buffer overflow in pngpread.c in libpng before 1.2.44 and 1.4.x before 1.4.3, as used in progressive applications, might allow remote attackers to execute arbitrary code via a PNG image that triggers an additional data row.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libpng12-0 1.2.15~beta5-3ubuntu0.2

References:

Source	Reference
APPLE	APPLE-SA-2010-08-24-1
APPLE	APPLE-SA-2010-11-10-1

Source	Reference
APPLE	APPLE-SA-2010-11-22-1
APPLE	APPLE-SA-2011-03-02-1
APPLE	APPLE-SA-2011-03-09-2
BID	41174
CVE	CVE-2010-1205
CVE	CVE-2010-2249
DEBIAN	DSA-2072
OVAL	OVAL11851
USN	USN-960-1
XF	59815
XF	59816

Vulnerability Solution:

- libpng12-0 on Ubuntu Linux 10.04
Upgrade libpng12-0 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 8.04
Upgrade libpng12-0 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 9.04
Upgrade libpng12-0 for Ubuntu 9.04
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 9.10
Upgrade libpng12-0 for Ubuntu 9.10
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version

3.1.91. USN-987-1: Samba vulnerability (ubuntu-usn-987-1)*Description:*

Stack-based buffer overflow in the (1) sid_parse and (2) dom_sid_parse functions in Samba before 3.5.5 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted Windows Security ID (SID) on a file share.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu samba 3.0.20-0.1ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
APPLE	APPLE-SA-2011-06-23-1
BID	43212
CVE	CVE-2010-3069
REDHAT	RHSA-2010:0860
USN	USN-987-1
XF	61773

Vulnerability Solution:

•samba on Ubuntu Linux 10.04

Upgrade samba for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade samba to the latest version

•samba on Ubuntu Linux 8.04

Upgrade samba for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade samba to the latest version

•samba on Ubuntu Linux 9.04

Upgrade samba for Ubuntu 9.04

Use `apt-get upgrade` to upgrade samba to the latest version

•samba on Ubuntu Linux 9.10

Upgrade samba for Ubuntu 9.10

Use `apt-get upgrade` to upgrade samba to the latest version

3.1.92. USN-989-1: PHP vulnerabilities (ubuntu-usn-989-1)*Description:*

Use-after-free vulnerability in the SplObjectStorage unserializer in PHP 5.2.x and 5.3.x through 5.3.2 allows remote attackers to execute arbitrary code or obtain sensitive information via serialized data, related to the PHP unserialize function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu php5-cli 5.2.4-2ubuntu5.10

References:

Source	Reference
--------	-----------

Source	Reference
APPLE	APPLE-SA-2010-08-24-1
APPLE	APPLE-SA-2010-11-10-1
APPLE	APPLE-SA-2011-03-21-1
BID	38430
BID	38431
BID	38708
BID	40948
CVE	CVE-2010-0397
CVE	CVE-2010-1128
CVE	CVE-2010-1129
CVE	CVE-2010-1130
CVE	CVE-2010-1866
CVE	CVE-2010-1868
CVE	CVE-2010-1917
CVE	CVE-2010-2094
CVE	CVE-2010-2225
CVE	CVE-2010-2531
CVE	CVE-2010-2950
CVE	CVE-2010-3065
DEBIAN	DSA-2089
DEBIAN	DSA-2266
REDHAT	RHSA-2010:0919
USN	USN-989-1
XF	58585
XF	59610

Vulnerability Solution:

- libapache2-mod-php5 on Ubuntu Linux 10.04
Upgrade libapache2-mod-php5 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- libapache2-mod-php5 on Ubuntu Linux 8.04
Upgrade libapache2-mod-php5 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- libapache2-mod-php5 on Ubuntu Linux 9.04
Upgrade libapache2-mod-php5 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version

- libapache2-mod-php5 on Ubuntu Linux 9.10
Upgrade libapache2-mod-php5 for Ubuntu 9.10
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- php5-cgi on Ubuntu Linux 10.04
Upgrade php5-cgi for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 8.04
Upgrade php5-cgi for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 9.04
Upgrade php5-cgi for Ubuntu 9.04
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 9.10
Upgrade php5-cgi for Ubuntu 9.10
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cli on Ubuntu Linux 10.04
Upgrade php5-cli for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade php5-cli to the latest version
- php5-cli on Ubuntu Linux 8.04
Upgrade php5-cli for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade php5-cli to the latest version
- php5-cli on Ubuntu Linux 9.04
Upgrade php5-cli for Ubuntu 9.04
Use `apt-get upgrade` to upgrade php5-cli to the latest version
- php5-cli on Ubuntu Linux 9.10
Upgrade php5-cli for Ubuntu 9.10
Use `apt-get upgrade` to upgrade php5-cli to the latest version

3.1.93. .rhosts files exist (unix-rhosts-file)

Description:

One or more .rhosts files were found on the system. The .rhosts file is used with the r- commands (rlogin, rsh, etc.) and it allows anyone to log in to the system without a password as long as they report having certain usernames or hostnames. The .rhosts authentication method should never be used, because it is very easy for an attacker to spoof his identity and log in to the system. Furthermore, the r- commands should be disabled -- the ssh protocol could be used instead where appropriate.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.0.102	The following .rhosts files were found./root/.rhosts/home/msfadmin/.rhosts

References:

None

Vulnerability Solution:

Delete all .rhosts files on the system. You should also make sure rshd and other r-commands are disabled.

3.2. Severe Vulnerabilities

3.2.1. Apache HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-0883) (apache-httpd-cve-2012-0883)

Description:

Insecure handling of LD_LIBRARY_PATH was found that could lead to the current working directory to be searched for DSOs. This could allow a local user to execute code as root if an administrator runs apachectl from an untrusted directory.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CVE	CVE-2012-0883
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

- Apache HTTPD >= 2.2 and < 2.2.23

Upgrade to Apache HTTPD version 2.2.23

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

- Apache HTTPD >= 2.4 and < 2.4.2

Upgrade to Apache HTTPD version 2.4.2

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.2.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually

customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.2. Apache HTTPD: mod_status buffer overflow (CVE-2014-0226) (apache-httpd-cve-2014-0226)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_status. Review your web server configuration for validation. A race condition was found in mod_status. An attacker able to access a public server status page on a server using a threaded MPM could send a carefully crafted request which could lead to a heap buffer overflow. Note that it is not a default or recommended configuration to have a public accessible server status page.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
BID	68678
CVE	CVE-2014-0226
DEBIAN	DSA-2989
DISA_SEVERITY	Category I
DISA_VMSKEY	V0053307
IAVM	2014-A-0114
OSVDB	109216
REDHAT	RHSA-2014:1019
REDHAT	RHSA-2014:1020
REDHAT	RHSA-2014:1021
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.29

Upgrade to Apache HTTPD version 2.2.29

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.29.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually

customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD ≥ 2.4 and $< 2.4.10$

Upgrade to Apache HTTPD version 2.4.10

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.10.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.3. Samba File Renaming Denial of Service Vulnerability (cifs-samba-file-renaming-dos)

Description:

smbd in Samba 3.0.6 through 3.0.23d allows remote authenticated users to cause a denial of service (memory and CPU exhaustion) by renaming a file in a way that prevents a request from being removed from the deferred open queue, which triggers an infinite loop.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:139	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian
192.168.0.102:445	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian

References:

Source	Reference
BID	22395
CVE	CVE-2007-0452
DEBIAN	DSA-1257
OSVDB	33100
OVAL	OVAL9758
REDHAT	RHSA-2007:0060
REDHAT	RHSA-2007:0061
SGI	20070201-01-P
SUSE	SUSE-SA:2007:016
URL	http://www.samba.org/samba/security/CVE-2007-0452.html
XF	32301

Vulnerability Solution:

Samba < 3.0.24

Download and apply the upgrade from: <https://ftp.samba.org/pub/samba/stable/samba-3.0.24.tar.gz>

Alternatively, patches may be available at <http://www.samba.org/samba/history/security.html>. Although Samba provides source code, it is recommended that you use your operating system's package manager to upgrade if possible. Please note that many operating system vendors choose to apply the most recent Samba security patches to their distributions without changing the package version to the most recent Samba version number. For the most reliable scan results, use correlation with authenticated scans.

3.2.4. SMB signing disabled (cifs-smb-signing-disabled)*Description:*

This system does not allow SMB signing. SMB signing allows the recipient of SMB packets to confirm their authenticity and helps prevent man in the middle attacks against SMB. SMB signing can be configured in one of three ways: disabled entirely (least secure), enabled, and required (most secure).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:139	Negotiate protocol response's security mode 3 indicates that SMB signing is disabled
192.168.0.102:445	Negotiate protocol response's security mode 3 indicates that SMB signing is disabled

References:

Source	Reference
URL	http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx

Vulnerability Solution:

•Microsoft Windows

Configure SMB signing for Windows

Configure the system to enable or require SMB signing as appropriate. The method and effect of doing this is system specific so please see [this TechNet article](#) for details. Note: ensure that SMB signing configuration is done for incoming connections (Server).

•Samba

Configure SMB signing for Samba

Configure Samba to enable or require SMB signing as appropriate. To enable SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:

```
server signing = auto
```

To require SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:

```
server signing = mandatory
```


3.2.5. FTP credentials transmitted unencrypted (ftp-plaintext-auth)

Description:

The server supports authentication methods in which credentials are sent in plaintext over unencrypted channels. If an attacker were to intercept traffic between a client and this server, the credentials would be exposed.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:21	Running FTP serviceConfiguration item ftp.plaintext.authentication set to 'true' matched

References:

None

Vulnerability Solution:

Disable plaintext authentication methods or enable encryption for the FTP service. Refer to the software's documentation for specific instructions.

3.2.6. PHP Multiple Vulnerabilities Fixed in version 5.2.5 (http-php-multiple-vulns-5-2-5)

Description:

PHP before 5.2.5 allows local users to bypass protection mechanisms configured through php_admin_value or php_admin_flag in httpd.conf by using ini_set to modify arbitrary configuration variables, a different issue than CVE-2006-4625.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2007-5898
CVE	CVE-2007-5899
CVE	CVE-2007-5900

Source	Reference
DEBIAN	DSA-1444
OSVDB	38918
OVAL	OVAL10080
OVAL	OVAL11211
REDHAT	RHSA-2008:0505
REDHAT	RHSA-2008:0544
REDHAT	RHSA-2008:0545
REDHAT	RHSA-2008:0546
REDHAT	RHSA-2008:0582
SUSE	SUSE-SA:2008:004
URL	http://www.php.net/releases/5_2_5.php

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.5.tar.gz>

3.2.7. No authentication for single user mode (lilo-linux-single-user-mode)*Description:*

Authorization is not enabled for the linux single user mode. This means that an attacker with physical access to the machine can enter single user mode (with root privileges) simply by typing 'linux single' at LILO prompt or at GRUB boot-editing menu. In Red Hat and Fedora this authorization is disabled by default to help users with lost root passwords. In any case this is a clear security risk.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Authentication not enabled for single user mode in /etc/inittab

References:

Source	Reference
BID	1005
CVE	CVE-2000-0219
URL	http://www.securityfocus.com/templates/archive.pike?list=1&msg=200002230248.NAA19185@cairo.anu.edu.au

Vulnerability Solution:

•Red Hat Linux >= 6, Oracle Linux >= 6, CentOS Linux >= 6

Enable authorization for linux single user mode

Refer to your vendor's documentation for exact details on enabling authorization for single user mode, however on RHEL 6+ and

variants this involves adding the following line to /etc/sysconfig/init:

```
SINGLE=/sbin/sulogin
```

- Enable authorization for linux single user mode

Refer to your vendor's documentation for exact details on enabling authorization for single user mode, however on systems that still use /etc/inittab, this involves adding the following line:

```
~:S:wait:/sbin/sulogin
```

3.2.8. ICMP redirection enabled (linux-icmp-redirect)

Description:

By default, many linux systems enable a feature called ICMP redirection, where the machine will alter its route table in response to an ICMP redirect message from any network device.

There is a risk that this feature could be used to subvert a host's routing table in order to compromise its security (e.g., tricking it into sending packets via a specific route where they may be sniffed or altered).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	The net.ipv4.conf.all.accept_redirects sysctl variable is set to 1, expected 0. The net.ipv4.conf.default.accept_redirects sysctl variable is set to 1, expected 0. The net.ipv4.conf.all.secure_redirects sysctl variable is set to 1, expected 0. The net.ipv4.conf.default.secure_redirects sysctl variable is set to 1, expected 0.

References:

Source	Reference
BID	6823
MSKB	293626
XF	cisco-ios-icmp-redirect(11306)

Vulnerability Solution:

Linux

Issue the following commands as root:

```
sysctl -w net.ipv4.conf.all.accept_redirects=0
sysctl -w net.ipv4.conf.default.accept_redirects=0
sysctl -w net.ipv4.conf.all.secure_redirects=0
```

```
sysctl -w net.ipv4.conf.default.secure_redirects=0
```

These settings can be added to /etc/sysctl.conf to make them permanent.

3.2.9. MySQL vio_verify_callback() Zero-Depth X.509 Certificate Vulnerability (mysql-vio_verify_callback-zero-depth-x-509-certificate)

Description:

The vio_verify_callback function in viosslfactories.c in MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41, when OpenSSL is used, accepts a value of zero for the depth of X.509 certificates, which allows man-in-the-middle attackers to spoof arbitrary SSL-based MySQL servers via a crafted certificate, as demonstrated by a certificate presented by a server linked against the yaSSL library.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2009-4028
OVAL	OVAL10940
OVAL	OVAL8510
REDHAT	RHSA-2010:0109
URL	http://bugs.mysql.com/bug.php?id=47320
URL	http://dev.mysql.com/doc/refman/5.0/en/news-5-0-88.html
URL	http://dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.88

Upgrade to Oracle MySQL version 5.0.88

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.41

Upgrade to Oracle MySQL version 5.1.41

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.10. Oracle MySQL Vulnerability: CVE-2009-5026 (oracle-mysql-cve-2009-5026)

Description:

The executable comment feature in MySQL 5.0.x before 5.0.93 and 5.1.x before 5.1.50, when running in certain slave configurations in which the slave is running a newer version than the master, allows remote attackers to execute arbitrary SQL commands via custom comments.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2009-5026

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.93

Upgrade to Oracle MySQL version 5.0.93

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.50

Upgrade to Oracle MySQL version 5.1.50

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.11. PHP Vulnerability: CVE-2007-4889 (php-cve-2007-4889)

Description:

The MySQL extension in PHP 5.2.4 and earlier allows remote attackers to bypass safe_mode and open_basedir restrictions via the MySQL (1) LOAD_FILE, (2) INTO DUMPFILE, and (3) INTO OUTFILE functions, a different issue than CVE-2007-3997.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8

Affected Nodes:	Additional Information:
	Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2007-4889
XF	36555

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.5.tar.gz>

3.2.12. PHP Vulnerability: CVE-2011-4718 (php-cve-2011-4718)*Description:*

Session fixation vulnerability in the Sessions subsystem in PHP before 5.5.2 allows remote attackers to hijack web sessions by specifying a session ID.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2011-4718

Vulnerability Solution:

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.13. USN-1009-1: GNU C Library vulnerabilities (ubuntu-usn-1009-1)*Description:*

ld.so in the GNU C Library (aka glibc or libc6) before 2.11.3, and 2.12.x before 2.12.2, does not properly restrict use of the LD_AUDIT environment variable to reference dynamic shared objects (DSOs) as audit objects, which allows local users to gain privileges by leveraging an unsafe DSO located in a trusted library directory, as demonstrated by libpcprofile.so.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libc6 2.7-10ubuntu5

References:

Source	Reference
BID	44154
BID	44347
CERT-VN	537223
CVE	CVE-2010-3847
CVE	CVE-2010-3856
DEBIAN	DSA-2122
REDHAT	RHSA-2010:0787
REDHAT	RHSA-2010:0793
REDHAT	RHSA-2010:0872
USN	USN-1009-1

Vulnerability Solution:

- libc6 on Ubuntu Linux 10.04
Upgrade libc6 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libc6 to the latest version
- libc6 on Ubuntu Linux 10.10
Upgrade libc6 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libc6 to the latest version
- libc6 on Ubuntu Linux 8.04
Upgrade libc6 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libc6 to the latest version
- libc6 on Ubuntu Linux 9.04
Upgrade libc6 for Ubuntu 9.04
Use `apt-get upgrade` to upgrade libc6 to the latest version
- libc6 on Ubuntu Linux 9.10
Upgrade libc6 for Ubuntu 9.10
Use `apt-get upgrade` to upgrade libc6 to the latest version

3.2.14. USN-1042-1: PHP vulnerabilities (ubuntu-usn-1042-1)*Description:*

The `utf8_decode` function in PHP before 5.3.4 does not properly handle non-shortest form UTF-8 encoding and ill-formed subsequences in UTF-8 data, which makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu php5-cli 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
APPLE	APPLE-SA-2011-10-12-3
BID	43926
BID	44605
BID	44718
BID	44723
BID	44727
BID	44889
BID	45119
BID	45668
CERT-VN	479900
CVE	CVE-2009-5016
CVE	CVE-2010-3436
CVE	CVE-2010-3709
CVE	CVE-2010-3710
CVE	CVE-2010-3870
CVE	CVE-2010-4156
CVE	CVE-2010-4409
CVE	CVE-2010-4645
REDHAT	RHSA-2010:0919
REDHAT	RHSA-2011:0195
REDHAT	RHSA-2011:0196
USN	USN-1042-1

Source	Reference
XF	64470

Vulnerability Solution:

- libapache2-mod-php5 on Ubuntu Linux 10.04
Upgrade libapache2-mod-php5 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- libapache2-mod-php5 on Ubuntu Linux 10.10
Upgrade libapache2-mod-php5 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- libapache2-mod-php5 on Ubuntu Linux 8.04
Upgrade libapache2-mod-php5 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- libapache2-mod-php5 on Ubuntu Linux 9.10
Upgrade libapache2-mod-php5 for Ubuntu 9.10
Use `apt-get upgrade` to upgrade libapache2-mod-php5 to the latest version
- php5-cgi on Ubuntu Linux 10.04
Upgrade php5-cgi for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 10.10
Upgrade php5-cgi for Ubuntu 10.10
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 8.04
Upgrade php5-cgi for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 9.10
Upgrade php5-cgi for Ubuntu 9.10
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cli on Ubuntu Linux 10.04
Upgrade php5-cli for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade php5-cli to the latest version
- php5-cli on Ubuntu Linux 10.10
Upgrade php5-cli for Ubuntu 10.10
Use `apt-get upgrade` to upgrade php5-cli to the latest version
- php5-cli on Ubuntu Linux 8.04
Upgrade php5-cli for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade php5-cli to the latest version
- php5-cli on Ubuntu Linux 9.10
Upgrade php5-cli for Ubuntu 9.10
Use `apt-get upgrade` to upgrade php5-cli to the latest version

3.2.15. USN-1102-1: tiff vulnerability (ubuntu-usn-1102-1)

Description:

Heap-based buffer overflow in the thunder (aka ThunderScan) decoder in tif_thunder.c in LibTIFF 3.9.4 and earlier allows remote attackers to execute arbitrary code via crafted THUNDER_2BITDELTAS data in a .tiff file that has an unexpected BitsPerSample value.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libtiff4 3.8.2-7ubuntu3.4

References:

Source	Reference
APPLE	APPLE-SA-2012-02-01-1
APPLE	APPLE-SA-2012-05-09-1
APPLE	APPLE-SA-2012-09-19-1
BID	46951
CVE	CVE-2011-1167
DEBIAN	DSA-2210
OSVDB	71256
REDHAT	RHSA-2011:0392
USN	USN-1102-1
XF	66247

Vulnerability Solution:

•libtiff4 on Ubuntu Linux 10.04

Upgrade libtiff4 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

•libtiff4 on Ubuntu Linux 10.10

Upgrade libtiff4 for Ubuntu 10.10

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

•libtiff4 on Ubuntu Linux 8.04

Upgrade libtiff4 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

•libtiff4 on Ubuntu Linux 9.10

Upgrade libtiff4 for Ubuntu 9.10

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

3.2.16. USN-1113-1: Postfix vulnerabilities (ubuntu-usn-1113-1)

Description:

The postfix.postinst script in the Debian GNU/Linux and Ubuntu postfix 2.5.5 package grants the postfix user write access to /var/spool/postfix/pid, which might allow local users to conduct symlink attacks that overwrite arbitrary files.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu postfix 2.5.1-2ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	46767
CERT-VN	555316
CVE	CVE-2009-2939
CVE	CVE-2011-0411
DEBIAN	DSA-2233
OSVDB	71021
REDHAT	RHSA-2011:0422
REDHAT	RHSA-2011:0423
USN	USN-1113-1
XF	65932

Vulnerability Solution:

- postfix on Ubuntu Linux 10.04
Upgrade postfix for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade postfix to the latest version
- postfix on Ubuntu Linux 10.10
Upgrade postfix for Ubuntu 10.10
Use `apt-get upgrade` to upgrade postfix to the latest version
- postfix on Ubuntu Linux 8.04
Upgrade postfix for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade postfix to the latest version
- postfix on Ubuntu Linux 9.10
Upgrade postfix for Ubuntu 9.10

Use `apt-get upgrade` to upgrade postfix to the latest version

3.2.17. USN-1131-1: Postfix vulnerability (ubuntu-usn-1131-1)

Description:

The SMTP server in Postfix before 2.5.13, 2.6.x before 2.6.10, 2.7.x before 2.7.4, and 2.8.x before 2.8.3, when certain Cyrus SASL authentication methods are enabled, does not create a new server handle after client authentication fails, which allows remote attackers to cause a denial of service (heap memory corruption and daemon crash) or possibly execute arbitrary code via an invalid AUTH command with one method followed by an AUTH command with a different method.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu postfix 2.5.1-2ubuntu1

References:

Source	Reference
BID	47778
CERT-VN	727230
CVE	CVE-2011-1720
DEBIAN	DSA-2233
OSVDB	72259
SUSE	SUSE-SA:2011:023
USN	USN-1131-1
XF	67359

Vulnerability Solution:

- postfix on Ubuntu Linux 10.04
Upgrade postfix for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade postfix to the latest version
- postfix on Ubuntu Linux 10.10
Upgrade postfix for Ubuntu 10.10
Use `apt-get upgrade` to upgrade postfix to the latest version
- postfix on Ubuntu Linux 11.04
Upgrade postfix for Ubuntu 11.04
Use `apt-get upgrade` to upgrade postfix to the latest version
- postfix on Ubuntu Linux 8.04
Upgrade postfix for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade postfix to the latest version

3.2.18. USN-1140-1: PAM vulnerabilities (ubuntu-usn-1140-1)

Description:

pam_namespace.c in the pam_namespace module in Linux-PAM (aka pam) before 1.1.3 uses the environment of the invoking application or service during execution of the namespace.init script, which might allow local users to gain privileges by running a setuid program that relies on the pam_namespace PAM check, as demonstrated by the sudo program.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libpam-modules 0.99.7.1-5ubuntu6

References:

Source	Reference
BID	34010
BID	46045
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
DISA_SEVERITY	Category I
DISA_VMSKEY	V0027158
IAVM	2011-A-0066
REDHAT	RHSA-2010:0819
REDHAT	RHSA-2010:0891
USN	USN-1140-1
XF	49110
XF	65035

Source	Reference
XF	65036

Vulnerability Solution:

- libpam-modules on Ubuntu Linux 10.04
Upgrade libpam-modules for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libpam-modules to the latest version
- libpam-modules on Ubuntu Linux 10.10
Upgrade libpam-modules for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libpam-modules to the latest version
- libpam-modules on Ubuntu Linux 11.04
Upgrade libpam-modules for Ubuntu 11.04
Use `apt-get upgrade` to upgrade libpam-modules to the latest version
- libpam-modules on Ubuntu Linux 8.04
Upgrade libpam-modules for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libpam-modules to the latest version

3.2.19. USN-1172-1: logrotate vulnerabilities (ubuntu-usn-1172-1)*Description:*

The `shred_file` function in `logrotate.c` in `logrotate` 3.7.9 and earlier might allow context-dependent attackers to execute arbitrary commands via shell metacharacters in a log filename, as demonstrated by a filename that is automatically constructed on the basis of a hostname or virtual machine name.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu logrotate 3.7.1-3

References:

Source	Reference
BID	47167
CVE	CVE-2011-1098
CVE	CVE-2011-1154
CVE	CVE-2011-1155
CVE	CVE-2011-1548
REDHAT	RHSA-2011:0407

Source	Reference
USN	USN-1172-1

Vulnerability Solution:

- logrotate on Ubuntu Linux 10.04
Upgrade logrotate for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade logrotate to the latest version
- logrotate on Ubuntu Linux 10.10
Upgrade logrotate for Ubuntu 10.10
Use `apt-get upgrade` to upgrade logrotate to the latest version
- logrotate on Ubuntu Linux 11.04
Upgrade logrotate for Ubuntu 11.04
Use `apt-get upgrade` to upgrade logrotate to the latest version
- logrotate on Ubuntu Linux 8.04
Upgrade logrotate for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade logrotate to the latest version

3.2.20. USN-1175-1: libpng vulnerabilities (ubuntu-usn-1175-1)*Description:*

Buffer overflow in libpng 1.0.x before 1.0.55, 1.2.x before 1.2.45, 1.4.x before 1.4.8, and 1.5.x before 1.5.4, when used by an application that calls the png_rgb_to_gray function but not the png_set_expand function, allows remote attackers to overwrite memory with an arbitrary amount of data, and possibly have unspecified other impact, via a crafted PNG image.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libpng12-0 1.2.15~beta5-3ubuntu0.2

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
APPLE	APPLE-SA-2012-05-09-1
BID	48474
BID	48618
BID	48660
CERT-VN	819894

Source	Reference
CVE	CVE-2011-2501
CVE	CVE-2011-2690
CVE	CVE-2011-2692
DEBIAN	DSA-2287
REDHAT	RHSA-2011:1103
REDHAT	RHSA-2011:1104
REDHAT	RHSA-2011:1105
USN	USN-1175-1
XF	68517
XF	68536
XF	68538

Vulnerability Solution:

- libpng12-0 on Ubuntu Linux 10.04
Upgrade libpng12-0 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 10.10
Upgrade libpng12-0 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 11.04
Upgrade libpng12-0 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 8.04
Upgrade libpng12-0 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version

3.2.21. USN-1237-1: PAM vulnerabilities (ubuntu-usn-1237-1)*Description:*

Untrusted search path vulnerability in pam_motd (aka the MOTD module) in libpam-modules before 1.1.3-2ubuntu2.1 on Ubuntu 11.10, before 1.1.2-2ubuntu8.4 on Ubuntu 11.04, before 1.1.1-4ubuntu2.4 on Ubuntu 10.10, before 1.1.1-2ubuntu5.4 on Ubuntu 10.04 LTS, and before 0.99.7.1-5ubuntu6.5 on Ubuntu 8.04 LTS, when using certain configurations such as "session optional pam_motd.so", allows local users to gain privileges by modifying the PATH environment variable to reference a malicious command, as demonstrated via uname.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libpam-modules 0.99.7.1-5ubuntu6

References:

Source	Reference
CVE	CVE-2011-3148
CVE	CVE-2011-3149
CVE	CVE-2011-3628
USN	USN-1237-1

Vulnerability Solution:

- libpam-modules on Ubuntu Linux 10.04
Upgrade libpam-modules for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libpam-modules to the latest version
- libpam-modules on Ubuntu Linux 10.10
Upgrade libpam-modules for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libpam-modules to the latest version
- libpam-modules on Ubuntu Linux 11.04
Upgrade libpam-modules for Ubuntu 11.04
Use `apt-get upgrade` to upgrade libpam-modules to the latest version
- libpam-modules on Ubuntu Linux 11.10
Upgrade libpam-modules for Ubuntu 11.10
Use `apt-get upgrade` to upgrade libpam-modules to the latest version
- libpam-modules on Ubuntu Linux 8.04
Upgrade libpam-modules for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libpam-modules to the latest version

3.2.22. USN-1378-1: PostgreSQL vulnerabilities (ubuntu-usn-1378-1)*Description:*

CRLF injection vulnerability in pg_dump in PostgreSQL 8.3.x before 8.3.18, 8.4.x before 8.4.11, 9.0.x before 9.0.7, and 9.1.x before 9.1.3 allows user-assisted remote attackers to execute arbitrary SQL commands via a crafted file containing object names with newlines, which are inserted into an SQL script that is used when the database is restored.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04

Affected Nodes:	Additional Information:
	Vulnerable software installed: Ubuntu postgresql-8.3 8.3.1-1

References:

Source	Reference
CVE	CVE-2012-0866
CVE	CVE-2012-0867
CVE	CVE-2012-0868
DEBIAN	DSA-2418
REDHAT	RHSA-2012:0677
REDHAT	RHSA-2012:0678
USN	USN-1378-1

Vulnerability Solution:

- postgresql-8.3 on Ubuntu Linux 8.04
Upgrade postgresql-8.3 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version
- postgresql-8.4 on Ubuntu Linux 10.04
Upgrade postgresql-8.4 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version
- postgresql-8.4 on Ubuntu Linux 10.10
Upgrade postgresql-8.4 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version
- postgresql-8.4 on Ubuntu Linux 11.04
Upgrade postgresql-8.4 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version
- postgresql-9.1 on Ubuntu Linux 11.10
Upgrade postgresql-9.1 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade postgresql-9.1 to the latest version

3.2.23. USN-1402-1: libpng vulnerability (ubuntu-usn-1402-1)*Description:*

Integer signedness error in the png_inflate function in pngutil.c in libpng before 1.4.10beta01, as used in Google Chrome before 17.0.963.83 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted PNG file, a different vulnerability than CVE-2011-3026.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libpng12-0 1.2.15~beta5-3ubuntu0.2

References:

Source	Reference
CVE	CVE-2011-3045
OVAL	OVAL14763
REDHAT	RHSA-2012:0488
USN	USN-1402-1

Vulnerability Solution:

- libpng12-0 on Ubuntu Linux 10.04
Upgrade libpng12-0 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 10.10
Upgrade libpng12-0 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 11.04
Upgrade libpng12-0 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 11.10
Upgrade libpng12-0 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 8.04
Upgrade libpng12-0 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version

3.2.24. USN-1416-1: tiff vulnerabilities (ubuntu-usn-1416-1)*Description:*

Multiple integer overflows in tiff_getimage.c in LibTIFF 3.9.4 allow remote attackers to execute arbitrary code via a crafted tile size in a TIFF file, which is not properly handled by the (1) gtTileSeparate or (2) gtStripSeparate function, leading to a heap-based buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libtiff4 3.8.2-7ubuntu3.4

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-1
APPLE	APPLE-SA-2012-09-19-2
BID	47338
BID	52891
CVE	CVE-2010-4665
CVE	CVE-2012-1173
DEBIAN	DSA-2447
DEBIAN	DSA-2552
OSVDB	81025
REDHAT	RHSA-2012:0468
USN	USN-1416-1
XF	74656

Vulnerability Solution:

- libtiff4 on Ubuntu Linux 10.04
Upgrade libtiff4 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libtiff4 to the latest version
- libtiff4 on Ubuntu Linux 10.10
Upgrade libtiff4 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libtiff4 to the latest version
- libtiff4 on Ubuntu Linux 11.04
Upgrade libtiff4 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade libtiff4 to the latest version
- libtiff4 on Ubuntu Linux 11.10
Upgrade libtiff4 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade libtiff4 to the latest version
- libtiff4 on Ubuntu Linux 8.04
Upgrade libtiff4 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libtiff4 to the latest version

3.2.25. USN-1417-1: libpng vulnerability (ubuntu-usn-1417-1)

Description:

The png_set_text_2 function in pngset.c in libpng 1.0.x before 1.0.59, 1.2.x before 1.2.49, 1.4.x before 1.4.11, and 1.5.x before 1.5.10 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted text chunk in a PNG image file, which triggers a memory allocation failure that is not properly handled, leading to a heap-based buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libpng12-0 1.2.15~beta5-3ubuntu0.2

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-1
APPLE	APPLE-SA-2012-09-19-2
BID	52830
CVE	CVE-2011-3048
DEBIAN	DSA-2446
OSVDB	80822
REDHAT	RHSA-2012:0523
USN	USN-1417-1
XF	74494

Vulnerability Solution:

- libpng12-0 on Ubuntu Linux 10.04
Upgrade libpng12-0 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 10.10
Upgrade libpng12-0 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 11.04
Upgrade libpng12-0 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 11.10
Upgrade libpng12-0 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade libpng12-0 to the latest version
- libpng12-0 on Ubuntu Linux 8.04
Upgrade libpng12-0 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libpng12-0 to the latest version

3.2.26. USN-1442-1: Sudo vulnerability (ubuntu-usn-1442-1)

Description:

sudo 1.6.x and 1.7.x before 1.7.9p1, and 1.8.x before 1.8.4p5, does not properly support configurations that use a netmask syntax, which allows local users to bypass intended command restrictions in opportunistic circumstances by executing a command on a host that has an IPv4 address.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu sudo 1.6.9p10-1ubuntu3

References:

Source	Reference
CVE	CVE-2012-2337
DEBIAN	DSA-2478
DISA_SEVERITY	Category II
DISA_VMSKEY	V0038876
IAVM	2013-B-0064
USN	USN-1442-1

Vulnerability Solution:

- sudo on Ubuntu Linux 10.04
Upgrade sudo for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo on Ubuntu Linux 11.04
Upgrade sudo for Ubuntu 11.04
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo on Ubuntu Linux 11.10
Upgrade sudo for Ubuntu 11.10
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo on Ubuntu Linux 12.04
Upgrade sudo for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo on Ubuntu Linux 8.04
Upgrade sudo for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade sudo to the latest version

- sudo-ldap on Ubuntu Linux 10.04
Upgrade sudo-ldap for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade sudo-ldap to the latest version
- sudo-ldap on Ubuntu Linux 11.04
Upgrade sudo-ldap for Ubuntu 11.04
Use `apt-get upgrade` to upgrade sudo-ldap to the latest version
- sudo-ldap on Ubuntu Linux 11.10
Upgrade sudo-ldap for Ubuntu 11.10
Use `apt-get upgrade` to upgrade sudo-ldap to the latest version
- sudo-ldap on Ubuntu Linux 12.04
Upgrade sudo-ldap for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade sudo-ldap to the latest version
- sudo-ldap on Ubuntu Linux 8.04
Upgrade sudo-ldap for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade sudo-ldap to the latest version

3.2.27. USN-1447-1: libxml2 vulnerability (ubuntu-usn-1447-1)

Description:

Off-by-one error in libxml2, as used in Google Chrome before 19.0.1084.46 and other products, allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libxml2 2.6.31.dfsg-2ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2013-09-18-2
APPLE	APPLE-SA-2013-10-22-8
BID	53540
CVE	CVE-2011-3102
DISA_SEVERITY	Category I
DISA_VMSKEY	V0036787
IAVM	2013-A-0031

Source	Reference
REDHAT	RHSA-2013:0217
USN	USN-1447-1

Vulnerability Solution:

•libxml2 on Ubuntu Linux 10.04

Upgrade libxml2 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version

•libxml2 on Ubuntu Linux 11.04

Upgrade libxml2 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libxml2 to the latest version

•libxml2 on Ubuntu Linux 11.10

Upgrade libxml2 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libxml2 to the latest version

•libxml2 on Ubuntu Linux 12.04

Upgrade libxml2 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version

•libxml2 on Ubuntu Linux 8.04

Upgrade libxml2 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version

3.2.28. USN-1451-1: OpenSSL vulnerabilities (ubuntu-usn-1451-1)*Description:*

Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted TLS packet that is not properly handled during a certain explicit IV calculation.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu openssl 0.9.8g-4ubuntu3

References:

Source	Reference
APPLE	APPLE-SA-2013-06-04-1
BID	53476
CERT-VN	737740

Source	Reference
CVE	CVE-2012-0884
CVE	CVE-2012-2333
DEBIAN	DSA-2454
DEBIAN	DSA-2475
REDHAT	RHSA-2012:0488
REDHAT	RHSA-2012:0531
REDHAT	RHSA-2012:1306
REDHAT	RHSA-2012:1307
REDHAT	RHSA-2012:1308
USN	USN-1451-1
XF	75525

Vulnerability Solution:

- libssl0.9.8 on Ubuntu Linux 10.04
Upgrade libssl0.9.8 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libssl0.9.8 to the latest version
- libssl0.9.8 on Ubuntu Linux 11.04
Upgrade libssl0.9.8 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade libssl0.9.8 to the latest version
- libssl0.9.8 on Ubuntu Linux 8.04
Upgrade libssl0.9.8 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libssl0.9.8 to the latest version
- libssl1.0.0 on Ubuntu Linux 11.10
Upgrade libssl1.0.0 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade libssl1.0.0 to the latest version
- libssl1.0.0 on Ubuntu Linux 12.04
Upgrade libssl1.0.0 for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade libssl1.0.0 to the latest version
- openssl on Ubuntu Linux 10.04
Upgrade openssl for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade openssl to the latest version
- openssl on Ubuntu Linux 11.04
Upgrade openssl for Ubuntu 11.04
Use `apt-get upgrade` to upgrade openssl to the latest version
- openssl on Ubuntu Linux 11.10
Upgrade openssl for Ubuntu 11.10
Use `apt-get upgrade` to upgrade openssl to the latest version
- openssl on Ubuntu Linux 12.04
Upgrade openssl for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade openssl to the latest version

- openssl on Ubuntu Linux 8.04

Upgrade openssl for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade openssl to the latest version

3.2.29. USN-1576-1: Dbus vulnerability (ubuntu-usn-1576-1)

Description:

libdbus 1.5.x and earlier, when used in setuid or other privileged programs in X.org and possibly other products, allows local users to gain privileges and execute arbitrary code via the DBUS_SYSTEM_BUS_ADDRESS environment variable. NOTE: libdbus maintainers state that this is a vulnerability in the applications that do not cleanse environment variables, not in libdbus itself: "we do not support use of libdbus in setuid binaries that do not sanitize their environment before their first call into libdbus."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libdbus-1-3 1.1.20-1ubuntu1

References:

Source	Reference
BID	55517
CVE	CVE-2012-3524
REDHAT	RHSA-2012:1261
USN	USN-1576-1

Vulnerability Solution:

- dbus on Ubuntu Linux 10.04

Upgrade dbus for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade dbus to the latest version
- dbus on Ubuntu Linux 11.04

Upgrade dbus for Ubuntu 11.04

Use `apt-get upgrade` to upgrade dbus to the latest version
- dbus on Ubuntu Linux 11.10

Upgrade dbus for Ubuntu 11.10

Use `apt-get upgrade` to upgrade dbus to the latest version
- dbus on Ubuntu Linux 12.04

Upgrade dbus for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade dbus to the latest version

- dbus on Ubuntu Linux 8.04

Upgrade dbus for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade dbus to the latest version

- libdbus-1-3 on Ubuntu Linux 10.04

Upgrade libdbus-1-3 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version

- libdbus-1-3 on Ubuntu Linux 11.04

Upgrade libdbus-1-3 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version

- libdbus-1-3 on Ubuntu Linux 11.10

Upgrade libdbus-1-3 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version

- libdbus-1-3 on Ubuntu Linux 12.04

Upgrade libdbus-1-3 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version

- libdbus-1-3 on Ubuntu Linux 8.04

Upgrade libdbus-1-3 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version

3.2.30. USN-1587-1: libxml2 vulnerability (ubuntu-usn-1587-1)

Description:

Multiple integer overflows in libxml2, as used in Google Chrome before 20.0.1132.43 and other products, on 64-bit Linux platforms allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libxml2 2.6.31.dfsg-2ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2013-09-18-2
APPLE	APPLE-SA-2013-10-22-8
BID	54718
CVE	CVE-2012-2807
DEBIAN	DSA-2521

Source	Reference
DISA_SEVERITY	Category I
DISA_VMSKEY	V0036787
IAVM	2013-A-0031
USN	USN-1587-1

Vulnerability Solution:

•libxml2 on Ubuntu Linux 10.04

Upgrade libxml2 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version

•libxml2 on Ubuntu Linux 11.04

Upgrade libxml2 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libxml2 to the latest version

•libxml2 on Ubuntu Linux 11.10

Upgrade libxml2 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libxml2 to the latest version

•libxml2 on Ubuntu Linux 12.04

Upgrade libxml2 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version

•libxml2 on Ubuntu Linux 8.04

Upgrade libxml2 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version

3.2.31. USN-1589-1: GNU C Library vulnerabilities (ubuntu-usn-1589-1)*Description:*

The `vfprintf` function in `stdio-common/vfprintf.c` in GNU C Library (aka glibc) 2.5, 2.12, and probably other versions does not "properly restrict the use of" the `alloca` function when allocating the SPECS array, which allows context-dependent attackers to bypass the FORTIFY_SOURCE format-string protection mechanism and cause a denial of service (crash) or possibly execute arbitrary code via a crafted format string using positional parameters and a large number of format specifiers, a different vulnerability than CVE-2012-3404 and CVE-2012-3405.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libc6 2.7-10ubuntu5

References:

Source	Reference
--------	-----------

Source	Reference
BID	54982
CVE	CVE-2012-3404
CVE	CVE-2012-3405
CVE	CVE-2012-3406
CVE	CVE-2012-3480
OSVDB	84710
REDHAT	RHSA-2012:1097
REDHAT	RHSA-2012:1098
REDHAT	RHSA-2012:1185
REDHAT	RHSA-2012:1200
REDHAT	RHSA-2012:1207
REDHAT	RHSA-2012:1208
REDHAT	RHSA-2012:1262
REDHAT	RHSA-2012:1325
USN	USN-1589-1

Vulnerability Solution:

- libc6 on Ubuntu Linux 10.04

Upgrade libc6 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libc6 to the latest version

- libc6 on Ubuntu Linux 11.04

Upgrade libc6 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libc6 to the latest version

- libc6 on Ubuntu Linux 11.10

Upgrade libc6 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libc6 to the latest version

- libc6 on Ubuntu Linux 12.04

Upgrade libc6 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libc6 to the latest version

- libc6 on Ubuntu Linux 8.04

Upgrade libc6 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libc6 to the latest version

3.2.32. USN-1613-1: Python 2.5 vulnerabilities (ubuntu-usn-1613-1)

Description:

Untrusted search path vulnerability in the PySys_SetArgv API function in Python 2.6 and earlier, and possibly later versions, prepends an empty string to sys.path when the argv[0] argument does not contain a path separator, which might allow local users to execute arbitrary code via a Trojan horse Python file in the current working directory.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu python2.5-minimal 2.5.2-2ubuntu6.1

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
APPLE	APPLE-SA-2013-10-22-3
BID	40370
BID	40863
BID	44533
BID	46541
BID	52379
BID	54083
CVE	CVE-2008-5983
CVE	CVE-2010-1634
CVE	CVE-2010-2089
CVE	CVE-2010-3493
CVE	CVE-2011-1015
CVE	CVE-2011-1521
CVE	CVE-2011-4940
CVE	CVE-2011-4944
CVE	CVE-2012-0845
CVE	CVE-2012-0876
CVE	CVE-2012-1148
DEBIAN	DSA-2525
DISA_SEVERITY	Category I
DISA_VMSKEY	V0031252
DISA_VMSKEY	V0035032

Source	Reference
IAVM	2012-A-0020
IAVM	2012-A-0189
OVAL	OVAL12210
REDHAT	RHSA-2011:0027
REDHAT	RHSA-2012:0731
USN	USN-1613-1

Vulnerability Solution:

- python2.5 on Ubuntu Linux 8.04
Upgrade python2.5 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade python2.5 to the latest version
- python2.5-minimal on Ubuntu Linux 8.04
Upgrade python2.5-minimal for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade python2.5-minimal to the latest version

3.2.33. USN-1631-1: LibTIFF vulnerabilities (ubuntu-usn-1631-1)*Description:*

ppm2tiff does not check the return value of the TIFFScanlineSize function, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PPM image that triggers an integer overflow, a zero-memory allocation, and a heap-based buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libtiff4 3.8.2-7ubuntu3.4

References:

Source	Reference
BID	55673
BID	56372
CVE	CVE-2012-4447
CVE	CVE-2012-4564
DEBIAN	DSA-2561
DEBIAN	DSA-2575

Source	Reference
DISA_SEVERITY	Category I
DISA_VMSKEY	V0036903
IAVM	2013-A-0048
OSVDB	86878
REDHAT	RHSA-2012:1590
USN	USN-1631-1
XF	79750

Vulnerability Solution:

•libtiff4 on Ubuntu Linux 10.04

Upgrade libtiff4 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

•libtiff4 on Ubuntu Linux 11.10

Upgrade libtiff4 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

•libtiff4 on Ubuntu Linux 12.04

Upgrade libtiff4 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

•libtiff4 on Ubuntu Linux 8.04

Upgrade libtiff4 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

•libtiff5 on Ubuntu Linux 12.10

Upgrade libtiff5 for Ubuntu 12.10

Use `apt-get upgrade` to upgrade libtiff5 to the latest version

3.2.34. USN-1655-1: LibTIFF vulnerability (ubuntu-usn-1655-1)*Description:*

Stack-based buffer overflow in tif_dir.c in LibTIFF before 4.0.2 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted DOTRANGE tag in a TIFF image.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libtiff4 3.8.2-7ubuntu3.4

References:

Source	Reference
BID	56715
CVE	CVE-2012-5581
REDHAT	RHSA-2012:1590
USN	USN-1655-1
XF	80339

Vulnerability Solution:

•libtiff4 on Ubuntu Linux 10.04

Upgrade libtiff4 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

•libtiff4 on Ubuntu Linux 11.10

Upgrade libtiff4 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

•libtiff4 on Ubuntu Linux 12.04

Upgrade libtiff4 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

•libtiff4 on Ubuntu Linux 8.04

Upgrade libtiff4 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libtiff4 to the latest version

3.2.35. USN-1656-1: Libxml2 vulnerability (ubuntu-usn-1656-1)*Description:*

Heap-based buffer underflow in the xmlParseAttValueComplex function in parser.c in libxml2 2.9.0 and earlier, as used in Google Chrome before 23.0.1271.91 and other products, allows remote attackers to cause a denial of service or possibly execute arbitrary code via crafted entities in an XML document.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libxml2 2.6.31.dfsg-2ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2013-09-18-2
APPLE	APPLE-SA-2013-10-22-8

Source	Reference
BID	56684
CVE	CVE-2012-5134
DEBIAN	DSA-2580
REDHAT	RHSA-2012:1512
REDHAT	RHSA-2013:0217
USN	USN-1656-1
XF	80294

Vulnerability Solution:

•libxml2 on Ubuntu Linux 10.04

Upgrade libxml2 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version

•libxml2 on Ubuntu Linux 11.10

Upgrade libxml2 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libxml2 to the latest version

•libxml2 on Ubuntu Linux 12.04

Upgrade libxml2 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version

•libxml2 on Ubuntu Linux 12.10

Upgrade libxml2 for Ubuntu 12.10

Use `apt-get upgrade` to upgrade libxml2 to the latest version

•libxml2 on Ubuntu Linux 8.04

Upgrade libxml2 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version

3.2.36. USN-1717-1: PostgreSQL vulnerability (ubuntu-usn-1717-1)*Description:*

PostgreSQL 9.2.x before 9.2.3, 9.1.x before 9.1.8, 9.0.x before 9.0.12, 8.4.x before 8.4.16, and 8.3.x before 8.3.23 does not properly declare the enum_recv function in backend/utils/adt/enum.c, which causes it to be invoked with incorrect arguments and allows remote authenticated users to cause a denial of service (server crash) or read sensitive process memory via a crafted SQL command, which triggers an array index error and an out-of-bounds read.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu postgresql-8.3 8.3.1-1

References:

Source	Reference
BID	57844
CVE	CVE-2013-0255
DEBIAN	DSA-2630
OSVDB	89935
REDHAT	RHSA-2013:1475
USN	USN-1717-1
XF	81917

Vulnerability Solution:

- postgresql-8.3 on Ubuntu Linux 8.04
Upgrade postgresql-8.3 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version
- postgresql-8.4 on Ubuntu Linux 10.04
Upgrade postgresql-8.4 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version
- postgresql-9.1 on Ubuntu Linux 11.10
Upgrade postgresql-9.1 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade postgresql-9.1 to the latest version
- postgresql-9.1 on Ubuntu Linux 12.04
Upgrade postgresql-9.1 for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade postgresql-9.1 to the latest version
- postgresql-9.1 on Ubuntu Linux 12.10
Upgrade postgresql-9.1 for Ubuntu 12.10
Use `apt-get upgrade` to upgrade postgresql-9.1 to the latest version

3.2.37. USN-1754-1: Sudo vulnerability (ubuntu-usn-1754-1)*Description:*

sudo 1.6.0 through 1.7.10p6 and sudo 1.8.0 through 1.8.6p6 allows local users or physically proximate attackers to bypass intended time restrictions and retain privileges without re-authenticating by setting the system clock and sudo user timestamp to the epoch.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu sudo 1.6.9p10-1ubuntu3

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CVE	CVE-2013-1775
DEBIAN	DSA-2642
OSVDB	90677
REDHAT	RHSA-2013:1353
REDHAT	RHSA-2013:1701
USN	USN-1754-1

Vulnerability Solution:

- sudo on Ubuntu Linux 10.04
Upgrade sudo for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo on Ubuntu Linux 11.10
Upgrade sudo for Ubuntu 11.10
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo on Ubuntu Linux 12.04
Upgrade sudo for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo on Ubuntu Linux 12.10
Upgrade sudo for Ubuntu 12.10
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo on Ubuntu Linux 8.04
Upgrade sudo for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo-ldap on Ubuntu Linux 10.04
Upgrade sudo-ldap for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade sudo-ldap to the latest version
- sudo-ldap on Ubuntu Linux 11.10
Upgrade sudo-ldap for Ubuntu 11.10
Use `apt-get upgrade` to upgrade sudo-ldap to the latest version
- sudo-ldap on Ubuntu Linux 12.04
Upgrade sudo-ldap for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade sudo-ldap to the latest version
- sudo-ldap on Ubuntu Linux 12.10
Upgrade sudo-ldap for Ubuntu 12.10
Use `apt-get upgrade` to upgrade sudo-ldap to the latest version
- sudo-ldap on Ubuntu Linux 8.04
Upgrade sudo-ldap for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade sudo-ldap to the latest version

3.2.38. USN-695-1: shadow vulnerability (ubuntu-usn-695-1)

Description:

/bin/login in shadow 4.0.18.1 in Debian GNU/Linux, and probably other Linux distributions, allows local users in the utmp group to overwrite arbitrary files via a symlink attack on a temporary file referenced in a line (aka ut_line) field in a utmp entry.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu login 1:4.0.18.2-1ubuntu2

References:

Source	Reference
BID	32552
CVE	CVE-2008-5394
OSVDB	52200
USN	USN-695-1
XF	47037

Vulnerability Solution:

- login on Ubuntu Linux 7.10
Upgrade login for Ubuntu 7.10
Use `apt-get upgrade` to upgrade login to the latest version
- login on Ubuntu Linux 8.04
Upgrade login for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade login to the latest version
- login on Ubuntu Linux 8.10
Upgrade login for Ubuntu 8.10
Use `apt-get upgrade` to upgrade login to the latest version

3.2.39. USN-722-1: sudo vulnerability (ubuntu-usn-722-1)

Description:

parse.c in sudo 1.6.9p17 through 1.6.9p19 does not properly interpret a system group (aka %group) in the sudoers file during authorization decisions for a user who belongs to that group, which allows local users to leverage an applicable sudoers file and gain root privileges via a sudo command.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu sudo 1.6.9p10-1ubuntu3

References:

Source	Reference
BID	33517
CVE	CVE-2009-0034
OSVDB	51736
OVAL	OVAL10856
OVAL	OVAL6462
REDHAT	RHSA-2009:0267
USN	USN-722-1

Vulnerability Solution:

- sudo on Ubuntu Linux 8.04
Upgrade sudo for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo on Ubuntu Linux 8.10
Upgrade sudo for Ubuntu 8.10
Use `apt-get upgrade` to upgrade sudo to the latest version

3.2.40. USN-726-1: curl vulnerability (ubuntu-usn-726-1)*Description:*

The redirect implementation in curl and libcurl 5.11 through 7.19.3, when CURLOPT_FOLLOWLOCATION is enabled, accepts arbitrary Location values, which might allow remote HTTP servers to (1) trigger arbitrary requests to intranet servers, (2) read or overwrite arbitrary files via a redirect to a file: URL, or (3) execute arbitrary commands via a redirect to an scp: URL.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libcurl3-gnutls 7.18.0-1ubuntu2

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
BID	33962
CVE	CVE-2009-0037
DEBIAN	DSA-1738
OVAL	OVAL11054
OVAL	OVAL6074
REDHAT	RHSA-2009:0341
USN	USN-726-1
XF	49030

Vulnerability Solution:

- libcurl3 on Ubuntu Linux 7.10
Upgrade libcurl3 for Ubuntu 7.10
Use `apt-get upgrade` to upgrade libcurl3 to the latest version
- libcurl3 on Ubuntu Linux 8.04
Upgrade libcurl3 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libcurl3 to the latest version
- libcurl3 on Ubuntu Linux 8.10
Upgrade libcurl3 for Ubuntu 8.10
Use `apt-get upgrade` to upgrade libcurl3 to the latest version
- libcurl3-gnutls on Ubuntu Linux 7.10
Upgrade libcurl3-gnutls for Ubuntu 7.10
Use `apt-get upgrade` to upgrade libcurl3-gnutls to the latest version
- libcurl3-gnutls on Ubuntu Linux 8.04
Upgrade libcurl3-gnutls for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libcurl3-gnutls to the latest version
- libcurl3-gnutls on Ubuntu Linux 8.10
Upgrade libcurl3-gnutls for Ubuntu 8.10
Use `apt-get upgrade` to upgrade libcurl3-gnutls to the latest version

3.2.41. USN-732-1: dash vulnerability (ubuntu-usn-732-1)*Description:*

Untrusted search path vulnerability in dash 0.5.4, when used as a login shell, allows local users to execute arbitrary code via a Trojan horse .profile file in the current working directory.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu dash 0.5.4-8ubuntu1

References:

Source	Reference
BID	34092
CVE	CVE-2009-0854
USN	USN-732-1
XF	49216

Vulnerability Solution:

- dash on Ubuntu Linux 8.04
Upgrade dash for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade dash to the latest version
- dash on Ubuntu Linux 8.10
Upgrade dash for Ubuntu 8.10
Use `apt-get upgrade` to upgrade dash to the latest version

3.2.42. USN-758-1: udev vulnerabilities (ubuntu-usn-758-1)*Description:*

udev before 1.4.1 does not verify whether a NETLINK message originates from kernel space, which allows local users to gain privileges by sending a NETLINK message from user space.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu udev 117-8

References:

Source	Reference
BID	34536
BID	34539
CVE	CVE-2009-1185

Source	Reference
CVE	CVE-2009-1186
DEBIAN	DSA-1772
OVAL	OVAL10925
OVAL	OVAL5975
REDHAT	RHSA-2009:0427
SUSE	SUSE-SA:2009:020
SUSE	SUSE-SA:2009:025
USN	USN-758-1

Vulnerability Solution:

•udev on Ubuntu Linux 7.10

Upgrade udev for Ubuntu 7.10

Use `apt-get upgrade` to upgrade udev to the latest version

•udev on Ubuntu Linux 8.04

Upgrade udev for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade udev to the latest version

•udev on Ubuntu Linux 8.10

Upgrade udev for Ubuntu 8.10

Use `apt-get upgrade` to upgrade udev to the latest version

3.2.43. USN-778-1: cron vulnerability (ubuntu-usn-778-1)*Description:*

do_command.c in Vixie cron (vixie-cron) 4.1 does not check the return code of a setuid call, which might allow local users to gain root privileges if setuid fails in cases such as PAM failures or resource limits, as originally demonstrated by a program that exceeds the process limits as defined in /etc/security/limits.conf.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu cron 3.0pl1-100ubuntu2

References:

Source	Reference
BID	18108
CVE	CVE-2006-2607

Source	Reference
OVAL	OVAL10213
REDHAT	RHSA-2006:0539
SUSE	SUSE-SA:2006:027
USN	USN-778-1
XF	26691

Vulnerability Solution:

•cron on Ubuntu Linux 8.04

Upgrade cron for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade cron to the latest version

•cron on Ubuntu Linux 8.10

Upgrade cron for Ubuntu 8.10

Use `apt-get upgrade` to upgrade cron to the latest version

•cron on Ubuntu Linux 9.04

Upgrade cron for Ubuntu 9.04

Use `apt-get upgrade` to upgrade cron to the latest version

3.2.44. USN-834-1: PostgreSQL vulnerabilities (ubuntu-usn-834-1)*Description:*

The core server component in PostgreSQL 8.3 before 8.3.8 and 8.2 before 8.2.14, when using LDAP authentication with anonymous binds, allows remote attackers to bypass authentication via an empty password.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu postgresql-8.3 8.3.1-1

References:

Source	Reference
BID	36314
CVE	CVE-2009-3229
CVE	CVE-2009-3230
CVE	CVE-2009-3231
DEBIAN	DSA-1900
OVAL	OVAL10166

Source	Reference
USN	USN-834-1

Vulnerability Solution:

- postgresql-8.3 on Ubuntu Linux 8.04
Upgrade postgresql-8.3 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version
- postgresql-8.3 on Ubuntu Linux 8.10
Upgrade postgresql-8.3 for Ubuntu 8.10
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version
- postgresql-8.3 on Ubuntu Linux 9.04
Upgrade postgresql-8.3 for Ubuntu 9.04
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version

3.2.45. USN-842-1: Wget vulnerability (ubuntu-usn-842-1)*Description:*

GNU Wget before 1.12 does not properly handle a '\0' character in a domain name in the Common Name field of an X.509 certificate, which allows man-in-the-middle remote attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu wget 1.10.2-3ubuntu1

References:

Source	Reference
BID	36205
CVE	CVE-2009-3490
OVAL	OVAL11099
USN	USN-842-1

Vulnerability Solution:

- wget on Ubuntu Linux 8.04
Upgrade wget for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade wget to the latest version
- wget on Ubuntu Linux 8.10
Upgrade wget for Ubuntu 8.10

Use `apt-get upgrade` to upgrade wget to the latest version

- wget on Ubuntu Linux 9.04

Upgrade wget for Ubuntu 9.04

Use `apt-get upgrade` to upgrade wget to the latest version

3.2.46. USN-876-1: PostgreSQL vulnerabilities (ubuntu-usn-876-1)

Description:

PostgreSQL 7.4.x before 7.4.27, 8.0.x before 8.0.23, 8.1.x before 8.1.19, 8.2.x before 8.2.15, 8.3.x before 8.3.9, and 8.4.x before 8.4.2 does not properly manage session-local state during execution of an index function by a database superuser, which allows remote authenticated users to gain privileges via a table with crafted index functions, as demonstrated by functions that modify (1) search_path or (2) a prepared statement, a related issue to CVE-2007-6600 and CVE-2009-3230.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu postgresql-8.3 8.3.1-1

References:

Source	Reference
BID	37333
BID	37334
CVE	CVE-2009-4034
CVE	CVE-2009-4136
OSVDB	61038
OSVDB	61039
OVAL	OVAL9358
REDHAT	RHSA-2010:0427
REDHAT	RHSA-2010:0428
REDHAT	RHSA-2010:0429
USN	USN-876-1

Vulnerability Solution:

- postgresql-8.3 on Ubuntu Linux 8.04

Upgrade postgresql-8.3 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version

- postgresql-8.3 on Ubuntu Linux 8.10
Upgrade postgresql-8.3 for Ubuntu 8.10
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version
- postgresql-8.3 on Ubuntu Linux 9.04
Upgrade postgresql-8.3 for Ubuntu 9.04
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version
- postgresql-8.4 on Ubuntu Linux 9.10
Upgrade postgresql-8.4 for Ubuntu 9.10
Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version

3.2.47. USN-889-1: gzip vulnerabilities (ubuntu-usn-889-1)

Description:

Integer underflow in the unlzv function in unlzv.c in gzip before 1.4 on 64-bit platforms, as used in ncompress and probably others, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted archive that uses LZV compression, leading to an array index error.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu gzip 1.3.12-3.2

References:

Source	Reference
APPLE	APPLE-SA-2010-11-10-1
CVE	CVE-2009-2624
CVE	CVE-2010-0001
DEBIAN	DSA-1974
DEBIAN	DSA-2074
OSVDB	61869
OVAL	OVAL10546
OVAL	OVAL7511
REDHAT	RHSA-2010:0061
REDHAT	RHSA-2010:0095
SUSE	SUSE-SA:2010:008
USN	USN-889-1

Vulnerability Solution:

•gzip on Ubuntu Linux 8.04

Upgrade gzip for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade gzip to the latest version

•gzip on Ubuntu Linux 8.10

Upgrade gzip for Ubuntu 8.10

Use `apt-get upgrade` to upgrade gzip to the latest version

•gzip on Ubuntu Linux 9.04

Upgrade gzip for Ubuntu 9.04

Use `apt-get upgrade` to upgrade gzip to the latest version

•gzip on Ubuntu Linux 9.10

Upgrade gzip for Ubuntu 9.10

Use `apt-get upgrade` to upgrade gzip to the latest version

3.2.48. USN-905-1: sudo vulnerabilities (ubuntu-usn-905-1)*Description:*

sudo 1.6.x before 1.6.9p21 and 1.7.x before 1.7.2p4, when a pseudo-command is enabled, permits a match between the name of the pseudo-command and the name of an executable file in an arbitrary directory, which allows local users to gain privileges via a crafted executable file, as demonstrated by a file named sudoedit in a user's home directory.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu sudo 1.6.9p10-1ubuntu3

References:

Source	Reference
BID	38362
CVE	CVE-2010-0426
CVE	CVE-2010-0427
DEBIAN	DSA-2006
OVAL	OVAL10814
OVAL	OVAL10946
OVAL	OVAL7216
OVAL	OVAL7238

Source	Reference
USN	USN-905-1

Vulnerability Solution:

•sudo on Ubuntu Linux 8.04

Upgrade sudo for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade sudo to the latest version

•sudo on Ubuntu Linux 8.10

Upgrade sudo for Ubuntu 8.10

Use `apt-get upgrade` to upgrade sudo to the latest version

•sudo on Ubuntu Linux 9.04

Upgrade sudo for Ubuntu 9.04

Use `apt-get upgrade` to upgrade sudo to the latest version

•sudo on Ubuntu Linux 9.10

Upgrade sudo for Ubuntu 9.10

Use `apt-get upgrade` to upgrade sudo to the latest version

•sudo-ldap on Ubuntu Linux 8.04

Upgrade sudo-ldap for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade sudo-ldap to the latest version

•sudo-ldap on Ubuntu Linux 8.10

Upgrade sudo-ldap for Ubuntu 8.10

Use `apt-get upgrade` to upgrade sudo-ldap to the latest version

•sudo-ldap on Ubuntu Linux 9.04

Upgrade sudo-ldap for Ubuntu 9.04

Use `apt-get upgrade` to upgrade sudo-ldap to the latest version

•sudo-ldap on Ubuntu Linux 9.10

Upgrade sudo-ldap for Ubuntu 9.10

Use `apt-get upgrade` to upgrade sudo-ldap to the latest version

3.2.49. USN-933-1: PostgreSQL vulnerability (ubuntu-usn-933-1)*Description:*

The bitsubstr function in backend/utils/adt/varbit.c in PostgreSQL 8.0.23, 8.1.11, and 8.3.8 allows remote authenticated users to cause a denial of service (daemon crash) or have unspecified other impact via vectors involving a negative integer in the third argument, as demonstrated by a SELECT statement that contains a call to the substring function for a bit string, related to an "overflow."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04

Affected Nodes:	Additional Information:
	Vulnerable software installed: Ubuntu postgresql-8.3 8.3.1-1

References:

Source	Reference
BID	37973
CVE	CVE-2010-0442
DEBIAN	DSA-2051
OVAL	OVAL9720
REDHAT	RHSA-2010:0427
REDHAT	RHSA-2010:0428
REDHAT	RHSA-2010:0429
USN	USN-933-1
XF	55902

Vulnerability Solution:

- postgresql-8.3 on Ubuntu Linux 8.04
Upgrade postgresql-8.3 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version
- postgresql-8.3 on Ubuntu Linux 9.04
Upgrade postgresql-8.3 for Ubuntu 9.04
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version
- postgresql-8.4 on Ubuntu Linux 9.10
Upgrade postgresql-8.4 for Ubuntu 9.10
Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version

3.2.50. USN-950-1: MySQL vulnerabilities (ubuntu-usn-950-1)*Description:*

Directory traversal vulnerability in MySQL 5.0 through 5.0.91 and 5.1 before 5.1.47 allows remote authenticated users to bypass intended table grants to read field definitions of arbitrary tables, and on 5.1 to read or delete content of arbitrary tables, via a .. (dot dot) in a table name.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu mysql-server-5.0 5.0.51a-3ubuntu5

References:

Source	Reference
APPLE	APPLE-SA-2010-11-10-1
BID	39543
BID	40257
CVE	CVE-2010-1621
CVE	CVE-2010-1626
CVE	CVE-2010-1848
CVE	CVE-2010-1849
CVE	CVE-2010-1850
OVAL	OVAL10258
OVAL	OVAL10846
OVAL	OVAL6693
OVAL	OVAL7210
OVAL	OVAL7328
OVAL	OVAL9490
REDHAT	RHSA-2010:0442
REDHAT	RHSA-2010:0824
USN	USN-950-1

Vulnerability Solution:

- mysql-server-5.0 on Ubuntu Linux 8.04
Upgrade mysql-server-5.0 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade mysql-server-5.0 to the latest version
- mysql-server-5.0 on Ubuntu Linux 9.04
Upgrade mysql-server-5.0 for Ubuntu 9.04
Use `apt-get upgrade` to upgrade mysql-server-5.0 to the latest version
- mysql-server-5.1 on Ubuntu Linux 10.04
Upgrade mysql-server-5.1 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade mysql-server-5.1 to the latest version
- mysql-server-5.1 on Ubuntu Linux 9.10
Upgrade mysql-server-5.1 for Ubuntu 9.10
Use `apt-get upgrade` to upgrade mysql-server-5.1 to the latest version

3.2.51. USN-954-1: tiff vulnerabilities (ubuntu-usn-954-1)*Description:*

Stack-based buffer overflow in the TIFFFetchSubjectDistance function in tif_dirread.c in LibTIFF before 3.9.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long EXIF SubjectDistance field in a TIFF file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libtiff4 3.8.2-7ubuntu3.4

References:

Source	Reference
APPLE	APPLE-SA-2010-06-15-1
APPLE	APPLE-SA-2010-06-16-1
BID	40823
CVE	CVE-2010-1411
CVE	CVE-2010-2065
CVE	CVE-2010-2067
OSVDB	65676
REDHAT	RHSA-2010:0519
REDHAT	RHSA-2010:0520
USN	USN-954-1

Vulnerability Solution:

- libtiff4 on Ubuntu Linux 10.04
Upgrade libtiff4 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libtiff4 to the latest version
- libtiff4 on Ubuntu Linux 8.04
Upgrade libtiff4 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libtiff4 to the latest version
- libtiff4 on Ubuntu Linux 9.04
Upgrade libtiff4 for Ubuntu 9.04
Use `apt-get upgrade` to upgrade libtiff4 to the latest version
- libtiff4 on Ubuntu Linux 9.10
Upgrade libtiff4 for Ubuntu 9.10
Use `apt-get upgrade` to upgrade libtiff4 to the latest version

3.2.52. USN-963-1: FreeType vulnerabilities (ubuntu-usn-963-1)

Description:

Multiple buffer overflows in demo programs in FreeType before 2.4.0 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libfreetype6 2.3.5-1ubuntu4.8.04.2

References:

Source	Reference
APPLE	APPLE-SA-2010-11-10-1
CVE	CVE-2010-2498
CVE	CVE-2010-2499
CVE	CVE-2010-2500
CVE	CVE-2010-2519
CVE	CVE-2010-2520
CVE	CVE-2010-2527
DEBIAN	DSA-2070
REDHAT	RHSA-2010:0577
REDHAT	RHSA-2010:0578
USN	USN-963-1

Vulnerability Solution:

- libfreetype6 on Ubuntu Linux 10.04

Upgrade libfreetype6 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

- libfreetype6 on Ubuntu Linux 8.04

Upgrade libfreetype6 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

- libfreetype6 on Ubuntu Linux 9.04

Upgrade libfreetype6 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

- libfreetype6 on Ubuntu Linux 9.10

Upgrade libfreetype6 for Ubuntu 9.10

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

3.2.53. USN-967-1: w3m vulnerability (ubuntu-usn-967-1)

Description:

istream.c in w3m 0.5.2 and possibly other versions, when ssl_verify_server is enabled, does not properly handle a '\0' character in a domain name in the (1) subject's Common Name or (2) Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu w3m 0.5.1-5.1ubuntu1

References:

Source	Reference
BID	40837
CVE	CVE-2010-2074
OSVDB	65538
REDHAT	RHSA-2010:0565
USN	USN-967-1

Vulnerability Solution:

•w3m on Ubuntu Linux 10.04

Upgrade w3m for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade w3m to the latest version

•w3m on Ubuntu Linux 8.04

Upgrade w3m for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade w3m to the latest version

•w3m on Ubuntu Linux 9.04

Upgrade w3m for Ubuntu 9.04

Use `apt-get upgrade` to upgrade w3m to the latest version

•w3m on Ubuntu Linux 9.10

Upgrade w3m for Ubuntu 9.10

Use `apt-get upgrade` to upgrade w3m to the latest version

3.2.54. USN-981-1: libwww-perl vulnerability (ubuntu-usn-981-1)

Description:

lwp-download in libwww-perl before 5.835 does not reject downloads to filenames that begin with a . (dot) character, which allows remote servers to create or overwrite files via (1) a 3xx redirect to a URL with a crafted filename or (2) a Content-Disposition header that suggests a crafted filename, and possibly execute arbitrary code as a consequence of writing to a dotfile in a home directory.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libwww-perl 5.808-1

References:

Source	Reference
CVE	CVE-2010-2253
USN	USN-981-1

Vulnerability Solution:

•libwww-perl on Ubuntu Linux 10.04

Upgrade libwww-perl for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libwww-perl to the latest version

•libwww-perl on Ubuntu Linux 8.04

Upgrade libwww-perl for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libwww-perl to the latest version

•libwww-perl on Ubuntu Linux 9.04

Upgrade libwww-perl for Ubuntu 9.04

Use `apt-get upgrade` to upgrade libwww-perl to the latest version

•libwww-perl on Ubuntu Linux 9.10

Upgrade libwww-perl for Ubuntu 9.10

Use `apt-get upgrade` to upgrade libwww-perl to the latest version

3.2.55. USN-982-1: Wget vulnerability (ubuntu-usn-982-1)

Description:

GNU Wget 1.12 and earlier uses a server-provided filename instead of the original URL to determine the destination filename of a download, which allows remote servers to create or overwrite arbitrary files via a 3xx redirect to a URL with a .wgetrc filename followed by a 3xx redirect to a URL with a crafted filename, and possibly execute arbitrary code as a consequence of writing to a dotfile in a home directory.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu wget 1.10.2-3ubuntu1

References:

Source	Reference
CVE	CVE-2010-2252
REDHAT	RHSA-2014:0151
USN	USN-982-1

Vulnerability Solution:

- wget on Ubuntu Linux 10.04
Upgrade wget for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade wget to the latest version
- wget on Ubuntu Linux 8.04
Upgrade wget for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade wget to the latest version
- wget on Ubuntu Linux 9.04
Upgrade wget for Ubuntu 9.04
Use `apt-get upgrade` to upgrade wget to the latest version
- wget on Ubuntu Linux 9.10
Upgrade wget for Ubuntu 9.10
Use `apt-get upgrade` to upgrade wget to the latest version

3.2.56. Anonymous root login is allowed (unix-anonymous-root-logins)*Description:*

Anonymous root logins should only be allowed from system console. `/etc/securetty` allows you to specify on which tty's and virtual consoles root is allowed to login. The tty and vc's listed in this file will allow root to login on certain tty's and VC's. On other tty or vc's root user will not be allowed and user has to "su" to become root.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Following entries in <code>/etc/securetty</code> may allow anonymous root logins: ttyS0tty0 xvc0hvc0pts/1pts/2pts/3pts/4pts/5pts/6pts/7pts/8pts/9pts/10pts/11pts/12pts/13 pts/14pts/15pts/16pts/17pts/18pts/19pts/20pts/21pts/22pts/23pts/24pts/25pts/26 pts/27pts/28pts/29pts/30pts/31pts/32pts/33pts/34pts/35pts/36pts/37pts/38pts/39 pts/40pts/41pts/42pts/43pts/44pts/45pts/46pts/47pts/48pts/49pts/50pts/51pts/52

Affected Nodes:	Additional Information:
	pts/53pts/54pts/55pts/56pts/57pts/58pts/59pts/60pts/61pts/62pts/63pts/64pts/65pts/66pts/67pts/68pts/69pts/70pts/71pts/72pts/73pts/74pts/75pts/76pts/77pts/78pts/79pts/80pts/81pts/82pts/83pts/84pts/85pts/86pts/87pts/88pts/89pts/90pts/91pts/92pts/93pts/94pts/95pts/96pts/97pts/98pts/99pts/100pts/101pts/102pts/103pts/104pts/105pts/106pts/107pts/108pts/109pts/110pts/111pts/112pts/113pts/114pts/115pts/116pts/117pts/118pts/119pts/120pts/121pts/122pts/123pts/124pts/125pts/126pts/127pts/128rshlogin

References:

None

Vulnerability Solution:

Remove all the entries in /etc/securetty except console, tty[0-9]* and vc\[0-9]*

Note: ssh does not use /etc/securetty. To disable root login through ssh, use the "PermitRootLogin" setting in /etc/ssh/sshd_config and restart the ssh daemon.

3.2.57. CIFS Share Writeable By Everyone (cifs-share-world-writeable)*Description:*

A share was found which allows write access by anyone. The impact of this vulnerability could include:

- Total system compromise (if the share point allows write access to critical system files)
- Untraceable modification of important data
- Denial of service by filling up the disk

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Successfully opened share "tmp" with write permissions.

References:

Source	Reference
CVE	CVE-1999-0520

Vulnerability Solution:

Adjust the share permissions to restrict access to only those members of the organization who need the data. It is considered bad practice to grant the "Everyone", "Guest", or "Authenticated Users" groups read or write access to a share.

3.2.58. SMB signing not required (cifs-smb-signing-not-required)*Description:*

This system enables, but does not require SMB signing. SMB signing allows the recipient of SMB packets to confirm their authenticity and helps prevent man in the middle attacks against SMB. SMB signing can be configured in one of three ways: disabled entirely (least secure), enabled, and required (most secure).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:139	Negotiate protocol response's security mode 3 indicates that SMB signing is not required
192.168.0.102:445	Negotiate protocol response's security mode 3 indicates that SMB signing is not required

References:

Source	Reference
URL	http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx

Vulnerability Solution:

•Microsoft Windows

Configure SMB signing for Windows

Configure the system to enable or require SMB signing as appropriate. The method and effect of doing this is system specific so please see [this TechNet article](#) for details. Note: ensure that SMB signing configuration is done for incoming connections (Server).

•Samba

Configure SMB signing for Samba

Configure Samba to enable or require SMB signing as appropriate. To enable SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:

```
server signing = auto
```

To require SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:

```
server signing = mandatory
```

3.2.59. ISC BIND: Key algorithm rollover bug in BIND 9 (CVE-2010-3614) (dns-bind-cve-2010-3614)

Description:

named in ISC BIND 9.x before 9.6.2-P3, 9.7.x before 9.7.2-P3, 9.4-ESV before 9.4-ESV-R4, and 9.6-ESV before 9.6-ESV-R3 does not properly determine the security status of an NS RRset during a DNSKEY algorithm rollover, which might allow remote attackers to cause a denial of service (DNSSEC validation error) by triggering a rollover.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	45137
CERT-VN	837744
CVE	CVE-2010-3614
DEBIAN	DSA-2130
OSVDB	69559
REDHAT	RHSA-2010:0975
REDHAT	RHSA-2010:0976
URL	https://kb.isc.org/article/AA-00936/0
URL	https://kb.isc.org/article/AA-00936/187/CVE-2010-3614%3A-Key-algorithm-rollover-bug-in-bind9.html

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the [ISC website](#).

3.2.60. HTTP TRACE Method Enabled (http-trace-method-enabled)*Description:*

The HTTP TRACE method is normally used to return the full HTTP request back to the requesting client for proxy-debugging purposes. An attacker can create a webpage using XMLHTTP, ActiveX, or XMLHttpRequest to cause a client to issue a TRACE request and capture the client's cookies. This effectively results in a Cross-Site Scripting attack.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceHTTP TRACE request to http://192.168.0.102/ 3: TRACE / HTTP/1.1 4: Host: 192.168.0.102 3: Cookie: vulnerable=yes

Affected Nodes:	Additional Information:

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
BID	15222
BID	19915
BID	24456
BID	36956
BID	9506
CERT-VN	867593
CVE	CVE-2004-2320
CVE	CVE-2004-2763
CVE	CVE-2005-3398
CVE	CVE-2006-4683
CVE	CVE-2007-3008
CVE	CVE-2008-7253
CVE	CVE-2009-2823
CVE	CVE-2010-0386
DISA_SEVERITY	Category II
DISA_VMSKEY	V0011706
IAVM	2005-T-0043
OSVDB	35511
OSVDB	3726
OVAL	OVAL1445
URL	http://www.apacheweek.com/issues/03-01-24#news
URL	http://www.kb.cert.org/vuls/id/867593
XF	14959
XF	34854

Vulnerability Solution:

•Apache HTTPD

Disable HTTP TRACE Method for Apache

Newer versions of Apache (1.3.34 and 2.0.55 and later) provide a configuration directive called TraceEnable. To deny TRACE requests, add the following line to the server configuration:

TraceEnable off

For older versions of the Apache webserver, use the mod_rewrite module to deny the TRACE requests:

RewriteEngine On

RewriteCond %{REQUEST_METHOD} ^TRACE

RewriteRule .* - [F]

- IIS, PWS, Microsoft-IIS, Internet Information Services, Internet Information Services, Microsoft-PWS

Disable HTTP TRACE Method for Microsoft IIS

For Microsoft Internet Information Services (IIS), you may use the URLScan tool, freely available at

<http://www.microsoft.com/technet/security/tools/urlscan.mspx>

- Java System Web Server, SunONE WebServer, Sun-ONE-Web-Server, iPlanet

Disable HTTP TRACE Method for SunONE/iPlanet

- For Sun ONE/iPlanet Web Server v6.0 SP2 and later, add the following configuration to the top of the default object in the 'obj.conf' file:

```
<Client method="TRACE">
```

```
AuthTrans fn="set-variable"
```

```
remove-headers="transfer-encoding"
```

```
set-headers="content-length: -1"
```

```
error="501"
```

```
</Client>
```

You must then restart the server for the changes to take effect.

- For Sun ONE/iPlanet Web Server prior to v6.0 SP2, follow the instructions provided the 'Relief/Workaround' section of Sun's official advisory: <http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603>

- Lotus Domino

Disable HTTP TRACE Method for Domino

Follow [IBM's instructions](#) for disabling HTTP methods on the Domino server by adding the following line to the server's NOTES.INI file:

HTTPDisableMethods=TRACE

After saving NOTES.INI, restart the Notes web server by issuing the console command "tell http restart".

3.2.61. MySQL Bug #29801: Remote Federated Engine Crash (mysql-bug-29801-remote-federated-engine-crash)

Description:

Versions of MySQL server before 5.0.52 and 5.1.23 suffer from a denial of service vulnerability via a flaw in the federated engine. On issuance of a command to a remote server (e.g., SHOW TABLE STATUS LIKE 'table'), the local federated server expects a query to contain fourteen columns. A response with less than fourteen columns causes the federated server to crash.

Affected Nodes:

--	--

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
URL	http://bugs.mysql.com/bug.php?id=29801

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.52

Upgrade to Oracle MySQL version 5.0.52

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.23

Upgrade to Oracle MySQL version 5.1.23

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.62. MySQL Bug #32707: send_error() Buffer Overflow Vulnerability (mysql-bug-32707-send-error-bof)*Description:*

A buffer overflow in MySQL 5.0 through 5.0.54 and 5.1 before 5.1.23 contains a flaw in the protocol layer. A long error message can cause a buffer overflow, potentially leading to execution of code.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
URL	http://bugs.mysql.com/bug.php?id=32707

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.54

Upgrade to Oracle MySQL version 5.0.54

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.23

Upgrade to Oracle MySQL version 5.1.23

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.63. MySQL Bug #37428: User-Defind Function Remote Code Execution (mysql-bug-37428-user-defind-function-remote-codex)

Description:

MySQL server 5.0 before 5.0.67 contains a flaw in creating and dropping certain functions. Using MySQL's user-defined functions, an authenticated attacker can create a function in a shared library and run arbitrary code against the server.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
URL	http://bugs.mysql.com/bug.php?id=37428

Vulnerability Solution:

Oracle MySQL >= 5.0 and < 5.0.67

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.64. MySQL Bug #38296: Nested Boolean Query Exhaustion Denial of Service (mysql-bug-38296-nested-boolean-query-exhaustion-dos)

Description:

There is a flaw in parsing queries in MySQL 5.0 before 5.0.68 and MySQL 5.1 before 5.1.28. An attacker can potentially cause the server to crash by sending a query with multiple nested logic operators, e.g. 'SELECT * FROM TABLE WHERE ... OR (... OR (... OR (...' etc.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
URL	http://bugs.mysql.com/bug.php?id=38296

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.68

Upgrade to Oracle MySQL version 5.0.68

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.28

Upgrade to Oracle MySQL version 5.1.28

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.65. Oracle MySQL Vulnerability: CVE-2012-0113 (oracle-mysql-cve-2012-0113)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect confidentiality and availability via unknown vectors, a different vulnerability than CVE-2012-0118.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0113
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.66. PHP Vulnerability: CVE-2010-1861 (php-cve-2010-1861)*Description:*

The sysvshm extension for PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to write to arbitrary memory addresses by using an object's __sleep function to interrupt an internal call to the shm_put_var function, which triggers access of a freed resource.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2010-1861

Vulnerability Solution:

- Upgrade to PHP version 5.2.14

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.14.tar.gz>

- Upgrade to PHP version 5.3.3

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.3.tar.gz>

3.2.67. PHP Vulnerability: CVE-2010-2191 (php-cve-2010-2191)*Description:*

The (1) parse_str, (2) preg_match, (3) unpack, and (4) pack functions; the (5) ZEND_FETCH_RW, (6) ZEND_CONCAT, and (7) ZEND_ASSIGN_CONCAT opcodes; and the (8) ArrayObject::uasort method in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler. NOTE: vectors 2 through 4 are related to the call time pass by reference feature.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2010-2191
XF	59221

Vulnerability Solution:

- Upgrade to PHP version 5.2.14
Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.14.tar.gz>
- Upgrade to PHP version 5.3.3
Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.3.tar.gz>

3.2.68. PHP Vulnerability: CVE-2012-1172 (php-cve-2012-1172)*Description:*

The file-upload implementation in rfc1867.c in PHP before 5.4.0 does not properly handle invalid [(open square bracket) characters in name values, which makes it easier for remote attackers to cause a denial of service (malformed \$_FILES indexes) or conduct directory traversal attacks during multi-file uploads by leveraging a script that lacks its own filename restrictions.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
CVE	CVE-2012-1172

Vulnerability Solution:

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.69. USN-1045-1: FUSE vulnerability (ubuntu-usn-1045-1)*Description:*

FUSE, possibly 2.8.5 and earlier, allows local users to create mtab entries with arbitrary pathnames, and consequently unmount any filesystem, via a symlink attack on the parent directory of the mountpoint of a FUSE filesystem, a different vulnerability than CVE-2010-0789.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu fuse-utils 2.7.2-1ubuntu2

References:

Source	Reference
BID	44623
CVE	CVE-2010-3879
OSVDB	70520
USN	USN-1045-1
XF	62986

Vulnerability Solution:

•fuse-utils on Ubuntu Linux 10.04

Upgrade fuse-utils for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade fuse-utils to the latest version

•fuse-utils on Ubuntu Linux 10.10

Upgrade fuse-utils for Ubuntu 10.10

Use `apt-get upgrade` to upgrade fuse-utils to the latest version

•fuse-utils on Ubuntu Linux 8.04

Upgrade fuse-utils for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade fuse-utils to the latest version

•fuse-utils on Ubuntu Linux 9.10

Upgrade fuse-utils for Ubuntu 9.10

Use `apt-get upgrade` to upgrade fuse-utils to the latest version

3.2.70. USN-1307-1: PHP vulnerability (ubuntu-usn-1307-1)

Description:

Integer overflow in the exif_process_IFD_TAG function in exif.c in the exif extension in PHP 5.4.0beta2 on 32-bit platforms allows remote attackers to read the contents of arbitrary memory locations or cause a denial of service via a crafted offset_val value in an EXIF header in a JPEG file, a different vulnerability than CVE-2011-0708.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu php5-cli 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2012-05-09-1
BID	50907
CVE	CVE-2011-4566
DEBIAN	DSA-2399
REDHAT	RHSA-2012:0019
REDHAT	RHSA-2012:0071
USN	USN-1307-1
XF	71612

Vulnerability Solution:

- php5-cgi on Ubuntu Linux 10.04
Upgrade php5-cgi for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 10.10
Upgrade php5-cgi for Ubuntu 10.10
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 11.04
Upgrade php5-cgi for Ubuntu 11.04
Use `apt-get upgrade` to upgrade php5-cgi to the latest version
- php5-cgi on Ubuntu Linux 11.10
Upgrade php5-cgi for Ubuntu 11.10

Use `apt-get upgrade` to upgrade php5-cgi to the latest version

- php5-cgi on Ubuntu Linux 8.04

Upgrade php5-cgi for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade php5-cgi to the latest version

- php5-cli on Ubuntu Linux 10.04

Upgrade php5-cli for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade php5-cli to the latest version

- php5-cli on Ubuntu Linux 10.10

Upgrade php5-cli for Ubuntu 10.10

Use `apt-get upgrade` to upgrade php5-cli to the latest version

- php5-cli on Ubuntu Linux 11.04

Upgrade php5-cli for Ubuntu 11.04

Use `apt-get upgrade` to upgrade php5-cli to the latest version

- php5-cli on Ubuntu Linux 11.10

Upgrade php5-cli for Ubuntu 11.10

Use `apt-get upgrade` to upgrade php5-cli to the latest version

- php5-cli on Ubuntu Linux 8.04

Upgrade php5-cli for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade php5-cli to the latest version

3.2.71. USN-1682-1: GnuPG vulnerability (ubuntu-usn-1682-1)

Description:

The read_block function in g10/import.c in GnuPG 1.4.x before 1.4.13 and 2.0.x through 2.0.19, when importing a key, allows remote attackers to corrupt the public keyring database or cause a denial of service (application crash) via a crafted length field of an OpenPGP packet.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu gnupg 1.4.6-2ubuntu5

References:

Source	Reference
BID	57102
CVE	CVE-2012-6085
REDHAT	RHSA-2013:1459

Source	Reference
USN	USN-1682-1
XF	80990

Vulnerability Solution:

- gnupg on Ubuntu Linux 10.04
Upgrade gnupg for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade gnupg to the latest version
- gnupg on Ubuntu Linux 11.10
Upgrade gnupg for Ubuntu 11.10
Use `apt-get upgrade` to upgrade gnupg to the latest version
- gnupg on Ubuntu Linux 12.04
Upgrade gnupg for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade gnupg to the latest version
- gnupg on Ubuntu Linux 12.10
Upgrade gnupg for Ubuntu 12.10
Use `apt-get upgrade` to upgrade gnupg to the latest version
- gnupg on Ubuntu Linux 8.04
Upgrade gnupg for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade gnupg to the latest version
- gnupg2 on Ubuntu Linux 10.04
Upgrade gnupg2 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade gnupg2 to the latest version
- gnupg2 on Ubuntu Linux 11.10
Upgrade gnupg2 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade gnupg2 to the latest version
- gnupg2 on Ubuntu Linux 12.04
Upgrade gnupg2 for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade gnupg2 to the latest version
- gnupg2 on Ubuntu Linux 12.10
Upgrade gnupg2 for Ubuntu 12.10
Use `apt-get upgrade` to upgrade gnupg2 to the latest version

3.2.72. USN-636-1: Postfix vulnerability (ubuntu-usn-636-1)*Description:*

Postfix before 2.3.15, 2.4 before 2.4.8, 2.5 before 2.5.4, and 2.6 before 2.6-20080814, when the operating system supports hard links to symlinks, allows local users to append e-mail messages to a file to which a root-owned symlink points, by creating a hard link to this symlink and then sending a message. NOTE: this can be leveraged to gain privileges if there is a symlink to an init script.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu postfix 2.5.1-2ubuntu1

References:

Source	Reference
BID	30691
CERT-VN	938323
CVE	CVE-2008-2936
DEBIAN	DSA-1629
OVAL	OVAL10033
REDHAT	RHSA-2008:0839
SUSE	SUSE-SA:2008:040
USN	USN-636-1
XF	44460

Vulnerability Solution:

- postfix on Ubuntu Linux 7.04
Upgrade postfix for Ubuntu 7.04
Use `apt-get upgrade` to upgrade postfix to the latest version
- postfix on Ubuntu Linux 7.10
Upgrade postfix for Ubuntu 7.10
Use `apt-get upgrade` to upgrade postfix to the latest version
- postfix on Ubuntu Linux 8.04
Upgrade postfix for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade postfix to the latest version

3.2.73. USN-704-1: OpenSSL vulnerability (ubuntu-usn-704-1)*Description:*

OpenSSL 0.9.8i and earlier does not properly check the return value from the EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu openssl 0.9.8g-4ubuntu3

References:

Source	Reference
APPLE	APPLE-SA-2009-05-12
BID	33150
CERT	TA09-133A
CVE	CVE-2008-5077
OVAL	OVAL6380
OVAL	OVAL9155
REDHAT	RHSA-2009:0004
USN	USN-704-1

Vulnerability Solution:

- libssl0.9.8 on Ubuntu Linux 7.10
Upgrade libssl0.9.8 for Ubuntu 7.10
Use `apt-get upgrade` to upgrade libssl0.9.8 to the latest version
- libssl0.9.8 on Ubuntu Linux 8.04
Upgrade libssl0.9.8 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libssl0.9.8 to the latest version
- libssl0.9.8 on Ubuntu Linux 8.10
Upgrade libssl0.9.8 for Ubuntu 8.10
Use `apt-get upgrade` to upgrade libssl0.9.8 to the latest version
- openssl on Ubuntu Linux 7.10
Upgrade openssl for Ubuntu 7.10
Use `apt-get upgrade` to upgrade openssl to the latest version
- openssl on Ubuntu Linux 8.04
Upgrade openssl for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade openssl to the latest version
- openssl on Ubuntu Linux 8.10
Upgrade openssl for Ubuntu 8.10
Use `apt-get upgrade` to upgrade openssl to the latest version

3.2.74. USN-953-1: fastjar vulnerability (ubuntu-usn-953-1)*Description:*

Directory traversal vulnerability in the `extract_jar` function in `jartool.c` in FastJar 0.98 allows remote attackers to create or overwrite arbitrary files via a `..` (dot dot) in a non-initial pathname component in a filename within a `.jar` archive, a related issue to CVE-2005-1080. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-3619.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu fastjar 2:0.95-1ubuntu2

References:

Source	Reference
BID	41006
CVE	CVE-2010-0831
OSVDB	65467
REDHAT	RHSA-2011:0025
USN	USN-953-1

Vulnerability Solution:

•fastjar on Ubuntu Linux 10.04

Upgrade fastjar for Ubuntu 10.04 LTS

Use ``apt-get upgrade`` to upgrade fastjar to the latest version

•fastjar on Ubuntu Linux 8.04

Upgrade fastjar for Ubuntu 8.04 LTS

Use ``apt-get upgrade`` to upgrade fastjar to the latest version

•fastjar on Ubuntu Linux 9.04

Upgrade fastjar for Ubuntu 9.04

Use ``apt-get upgrade`` to upgrade fastjar to the latest version

•fastjar on Ubuntu Linux 9.10

Upgrade fastjar for Ubuntu 9.10

Use ``apt-get upgrade`` to upgrade fastjar to the latest version

3.2.75. USN-956-1: sudo vulnerability (ubuntu-usn-956-1)

Description:

The secure path feature in `env.c` in `sudo` 1.3.1 through 1.6.9p22 and 1.7.0 through 1.7.2p6 does not properly handle an environment that contains multiple `PATH` variables, which might allow local users to gain privileges via a crafted value of the last `PATH` variable.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu sudo 1.6.9p10-1ubuntu3

References:

Source	Reference
BID	40538
CVE	CVE-2010-1646
DEBIAN	DSA-2062
OSVDB	65083
OVAL	OVAL10580
OVAL	OVAL7338
REDHAT	RHSA-2010:0475
USN	USN-956-1

Vulnerability Solution:

- sudo on Ubuntu Linux 10.04
Upgrade sudo for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo on Ubuntu Linux 8.04
Upgrade sudo for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo on Ubuntu Linux 9.04
Upgrade sudo for Ubuntu 9.04
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo on Ubuntu Linux 9.10
Upgrade sudo for Ubuntu 9.10
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo-ldap on Ubuntu Linux 10.04
Upgrade sudo-ldap for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade sudo-ldap to the latest version
- sudo-ldap on Ubuntu Linux 8.04
Upgrade sudo-ldap for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade sudo-ldap to the latest version
- sudo-ldap on Ubuntu Linux 9.04
Upgrade sudo-ldap for Ubuntu 9.04
Use `apt-get upgrade` to upgrade sudo-ldap to the latest version

- sudo-ldap on Ubuntu Linux 9.10

Upgrade sudo-ldap for Ubuntu 9.10

Use `apt-get upgrade` to upgrade sudo-ldap to the latest version

3.2.76. USN-990-2: Apache vulnerability (ubuntu-usn-990-2)

Description:

The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu apache2.2-common 2.2.8-1ubuntu0.15

References:

Source	Reference
APPLE	APPLE-SA-2010-01-19-1
APPLE	APPLE-SA-2010-05-18-1
APPLE	APPLE-SA-2010-05-18-2
BID	36935
CERT	TA10-222A
CERT	TA10-287A
CERT-VN	120541
CVE	CVE-2009-3555
DEBIAN	DSA-1934
DEBIAN	DSA-2141
DISA_SEVERITY	Category I
DISA_VMSKEY	V0027158
IAVM	2011-A-0066
MS	MS10-049

Source	Reference
OSVDB	60521
OSVDB	60972
OSVDB	62210
OSVDB	65202
OVAL	OVAL10088
OVAL	OVAL11578
OVAL	OVAL11617
OVAL	OVAL7315
OVAL	OVAL7478
OVAL	OVAL7973
OVAL	OVAL8366
OVAL	OVAL8535
REDHAT	RHSA-2010:0119
REDHAT	RHSA-2010:0130
REDHAT	RHSA-2010:0155
REDHAT	RHSA-2010:0165
REDHAT	RHSA-2010:0167
REDHAT	RHSA-2010:0337
REDHAT	RHSA-2010:0338
REDHAT	RHSA-2010:0339
REDHAT	RHSA-2010:0768
REDHAT	RHSA-2010:0770
REDHAT	RHSA-2010:0786
REDHAT	RHSA-2010:0807
REDHAT	RHSA-2010:0865
REDHAT	RHSA-2010:0986
REDHAT	RHSA-2010:0987
REDHAT	RHSA-2011:0880
SUSE	SUSE-SA:2009:057
SUSE	SUSE-SA:2010:061
USN	USN-990-2
XF	54158

Vulnerability Solution:

•apache2.2-common on Ubuntu Linux 10.04

Upgrade apache2.2-common for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade apache2.2-common to the latest version

•apache2.2-common on Ubuntu Linux 8.04

Upgrade apache2.2-common for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade apache2.2-common to the latest version

•apache2.2-common on Ubuntu Linux 9.04

Upgrade apache2.2-common for Ubuntu 9.04

Use `apt-get upgrade` to upgrade apache2.2-common to the latest version

•apache2.2-common on Ubuntu Linux 9.10

Upgrade apache2.2-common for Ubuntu 9.10

Use `apt-get upgrade` to upgrade apache2.2-common to the latest version

3.2.77. /etc/hosts.equiv allows remote access from some systems (unix-hosts-equiv-allows-access)*Description:*

The file /etc/hosts.equiv contains at least one entry that allows unauthenticated remote access from certain systems based only on the IP address or hostname. Not only is IP/host information easily hijacked by an attacker, but allowing users from certain hosts to log in without authenticating means anyone who gains access to the remote system can log in to your system.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	/etc/hosts.equiv contains 1 positive access entries

References:

None

Vulnerability Solution:

The /etc/hosts.equiv file should never be used. Remove the file. After removing the file create a symlink from that file to /dev/null, so that attackers cannot append to it:

```
rm /etc/hosts.equiv && ln -s /dev/null /etc/hosts.equiv
```

3.2.78. Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368) (apache-httpd-cve-2011-3368)*Description:*

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy. Review your web server configuration for validation. An exposure was found when using mod_proxy in reverse proxy mode. In certain configurations using RewriteRule with proxy flag, a remote attacker could cause the reverse proxy to connect to an arbitrary server, possibly disclosing sensitive information from internal web servers not directly accessible to attacker. No update of 1.3 will be released. Patches will be published to http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
BID	49957
CVE	CVE-2011-3368
OSVDB	76079
REDHAT	RHSA-2011:1391
REDHAT	RHSA-2011:1392
URL	http://httpd.apache.org/security/vulnerabilities_13.html
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	70336

Vulnerability Solution:

•Apache HTTPD >= 1.3 and < 2

Apply the patch for CVE-2011-3368 to 1.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/

No update of 1.3 will be released. Patches will be published to http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/

•Apache HTTPD >= 2.0 and < 2.0.65

Upgrade to Apache HTTPD version 2.0.65

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.2 and < 2.2.22

Upgrade to Apache HTTPD version 2.2.22

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.79. Apache HTTPD: HTTP Trailers processing bypass (CVE-2013-5704) (apache-httpd-cve-2013-5704)

Description:

HTTP trailers could be used to replace HTTP headers late during request processing, potentially undoing or otherwise confusing modules that examined or modified request headers earlier. This fix adds the "MergeTrailers" directive to restore legacy behavior.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
CVE	CVE-2013-5704
REDHAT	RHSA-2015:0325
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.29

Upgrade to Apache HTTPD version 2.2.29

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.29.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.12

Upgrade to Apache HTTPD version 2.4.12

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.12.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.80. Apache HTTPD: mod_dav crash (CVE-2013-6438) (apache-httpd-cve-2013-6438)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_dav. Review your web server configuration for validation. XML parsing code in mod_dav incorrectly calculates the end of the string when removing leading

spaces and places a NUL character outside the buffer, causing random crashes. This XML parsing code is only used with DAV provider modules that support DeltaV, of which the only publicly released provider is mod_dav_svn.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
APPLE	APPLE-SA-2014-10-16-1
APPLE	APPLE-SA-2015-04-08-2
BID	66303
CVE	CVE-2013-6438
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.27

Upgrade to Apache HTTPD version 2.2.27

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.27.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.9

Upgrade to Apache HTTPD version 2.4.9

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.9.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.81. Apache HTTPD: mod_log_config crash (CVE-2014-0098) (apache-httpd-cve-2014-0098)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_log_config. Review your web server configuration for validation. A flaw was found in mod_log_config. A remote attacker could send a specific truncated cookie causing a crash. This crash would only be a denial of service if using a threaded MPM.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
APPLE	APPLE-SA-2014-10-16-1
APPLE	APPLE-SA-2015-04-08-2
BID	66303
CVE	CVE-2014-0098
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.27

Upgrade to Apache HTTPD version 2.2.27

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.27.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.9

Upgrade to Apache HTTPD version 2.4.9

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.9.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.82. Apache HTTPD: mod_cgid denial of service (CVE-2014-0231) (apache-httpd-cve-2014-0231)*Description:*

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_cgid. Review your web server configuration for validation. A flaw was found in mod_cgid. If a server using mod_cgid hosted CGI scripts which did not consume standard input, a remote attacker could cause child processes to hang indefinitely, leading to denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
BID	68742
CVE	CVE-2014-0231
DEBIAN	DSA-2989
DISA_SEVERITY	Category I
DISA_VMSKEY	V0053307
IAVM	2014-A-0114
REDHAT	RHSA-2014:1019
REDHAT	RHSA-2014:1020
REDHAT	RHSA-2014:1021
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.29

Upgrade to Apache HTTPD version 2.2.29

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.29.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.10

Upgrade to Apache HTTPD version 2.4.10

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.10.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.83. Apache Tomcat default installation/welcome page installed (apache-tomcat-default-install-page)*Description:*

The Tomcat default installation or "Welcome" page is installed on this server. This usually indicates a newly installed server which has not yet been configured properly and which may not be known about.

In many cases, Tomcat is installed along with other applications and the user may not be aware that the web server is running. These servers are rarely patched and rarely monitored, providing hackers with a convenient target that is not likely to trip any alarms.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:8180	<p>Running HTTP serviceProduct Tomcat exists -- Apache TomcatHTTP GET request to http://192.168.0.102:8180/</p> <p>HTTP response code was an expected 200</p> <p>194: <td style="width:20px">&nbsp;</td></p> <p>195:</p> <p>196: <!-- Body --></p> <p>197: <td align="left" valign="top"></p> <p>194: ... means you've setup Tomcat successfully. Congratulations!</p></p>

References:

Source	Reference
OSVDB	2117

Vulnerability Solution:

If this server is required to provide necessary functionality, then the default page should be replaced with relevant content. Otherwise, this server should be removed from the network, following the security principle of minimum complexity.

3.2.84. Anonymous users can obtain the Windows password policy (cifs-nt-0002)

Description:

Anonymous users can obtain the Windows password policy from the system by using CIFS NULL sessions. The password policy contains sensitive information about minimum password length, password lockout threshold, password lockout duration, etc.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Retrieved domain policy for the METASPLOITABLE domain, with SID S-1-5-21-1042354039-2475377354-766472396

References:

Source	Reference
BID	959
CVE	CVE-2000-1200

Source	Reference
XF	4015

Vulnerability Solution:

•Microsoft Windows 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003

Disable NULL sessions for Windows 2003

Modify the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\

with the following values:

Value Name: RestrictAnonymous

Data Type: REG_DWORD

Data Value: 1

Value Name: RestrictAnonymousSAM

Data Type: REG_DWORD

Data Value: 1

Value Name: EveryoneIncludesAnonymous

Data Type: REG_DWORD

Data Value: 0

and set the following value to 0 (or, alternatively, delete it):

Value Name: TurnOffAnonymousBlock

Data Type: REG_DWORD

Data Value: 0

Modify the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\

with the following values:

Value Name: RestrictNullSessAccess

Data Type: REG_DWORD

Data Value: 1

Value Name: NullSessionPipes

Data Type: REG_MULTI_SZ

Data Value: "" (empty string, without quotes)

Open Local Security Settings, and disable the following setting:

Security Settings -> Local Policies -> Security Options ->

Network access: Allow anonymous SID/Name translation: Disabled

Finally, reboot the machine.

Please note that disabling NULL sessions may have an adverse impact on functionality, as some applications and network environments may depend on them for proper operation. Refer to [Microsoft Knowledge Base Article 823659](#) for more information.

•Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional

Disable NULL sessions for Windows XP

Modify the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\

with the following values:

Value Name: RestrictAnonymous

Data Type: REG_DWORD

Data Value: 1

Value Name: RestrictAnonymousSAM

Data Type: REG_DWORD

Data Value: 1

Value Name: EveryoneIncludesAnonymous

Data Type: REG_DWORD

Data Value: 0

Modify the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\

with the following values:

Value Name: RestrictNullSessAccess

Data Type: REG_DWORD

Data Value: 1

Value Name: NullSessionPipes

Data Type: REG_MULTI_SZ

Data Value: "" (empty string, without quotes)

Open Local Security Settings, and disable the following setting:

Security Settings -> Local Policies -> Security Options ->

Network access: Allow anonymous SID/Name translation: Disabled

Finally, reboot the machine.

Please note that disabling NULL sessions may have an adverse impact on functionality, as some applications and network environments may depend on them for proper operation. Refer to [Microsoft Knowledge Base Article Q246261](#) for more information.

- Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server

Disable NULL sessions for Windows 2000

Modify the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\

with the following value:

Value Name: RestrictAnonymous

Data Type: REG_DWORD

Data Value: 2

After modifying the registry, reboot the machine.

Please note that disabling NULL sessions may have an adverse impact on functionality, as some applications and network environments may depend on them for proper operation. Refer to [Microsoft Knowledge Base Article Q246261](https://support.microsoft.com/kb/q246261) for more information.

- Microsoft Windows NT Server 4.0, Microsoft Windows NT Server, Enterprise Edition 4.0, Microsoft Windows NT Workstation 4.0

Install Microsoft service pack Windows NT4 Service Pack 4

Download and apply the upgrade from: <http://support.microsoft.com/sp>

- Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition

Disable NULL sessions for Windows NT

Modify the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\

with the following value:

Value Name: RestrictAnonymous

Data Type: REG_DWORD

Data Value: 1

After modifying the registry, reboot the machine.

It is important to note that on Windows NT 4.0 systems, setting this registry entry will still leave the system open to various attacks, including brute-force enumeration of users and groups. A complete solution for Windows NT 4.0 systems is not available.

- Samba on Linux

Restrict anonymous access

To restrict anonymous access to Samba, modify your "smb.conf" settings as follows:

guest account = nobody

restrict anonymous = 1

Note: Make sure you do NOT list a user "nobody" in your password file.

•Novell NetWare

Novell Network CIFS

As of May 9, 2007 Novell Network CIFS does not provide a workaround for this vulnerability.

3.2.85. Samba Connection Flooding Denial of Service Vulnerability (cifs-samba-connection-flooding-dos)

Description:

The smdb daemon (smbd/service.c) in Samba 3.0.1 through 3.0.22 allows remote attackers to cause a denial of service (memory consumption) via a large number of share connection requests.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:139	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian
192.168.0.102:445	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian

References:

Source	Reference
APPLE	APPLE-SA-2006-11-28
BID	18927
CERT	TA06-333A
CERT-VN	313836
CVE	CVE-2006-3403
DEBIAN	DSA-1110
OVAL	OVAL11355
REDHAT	RHSA-2006:0591
SGI	20060703-01-P
URL	http://www.samba.org/samba/security/CVE-2006-3403.html
XF	27648

Vulnerability Solution:

Samba < 3.0.23

Download and apply the upgrade from: <https://ftp.samba.org/pub/samba/stable/samba-3.0.23.tar.gz>

Alternatively, patches may be available at <http://www.samba.org/samba/history/security.html>. Although Samba provides source code, it is recommended that you use your operating system's package manager to upgrade if possible. Please note that many operating system vendors choose to apply the most recent Samba security patches to their distributions without changing the package version to the most recent Samba version number. For the most reliable scan results, use correlation with authenticated scans.

3.2.86. DNS server allows cache snooping (dns-allows-cache-snooping)

Description:

This DNS server is susceptible to DNS cache snooping, whereby an attacker can make non-recursive queries to a DNS server, looking for records potentially already resolved by this DNS server for other clients. Depending on the response, an attacker can use this information to potentially launch other attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:53	Received 2 answers to a non-recursive query for www.rapid7.com
192.168.0.102:53	Received 2 answers to a non-recursive query for www.rapid7.com

References:

Source	Reference
URL	http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf

Vulnerability Solution:

Restrict the processing of DNS queries to only systems that should be allowed to use this nameserver.

3.2.87. ISC BIND: BIND 9 Resolver crashes after logging an error in query.c (CVE-2011-4313) (dns-bind-cve-2011-4313)

Description:

query.c in ISC BIND 9.0.x through 9.6.x, 9.4-ESV through 9.4-ESV-R5, 9.6-ESV through 9.6-ESV-R5, 9.7.0 through 9.7.4, 9.8.0 through 9.8.1, and 9.9.0a1 through 9.9.0b1 allows remote attackers to cause a denial of service (assertion failure and named exit) via unknown vectors related to recursive DNS queries, error logging, and the caching of an invalid record by the resolver.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
BID	50690

Source	Reference
CERT-VN	606539
CVE	CVE-2011-4313
DEBIAN	DSA-2347
OSVDB	77159
OVAL	OVAL14343
REDHAT	RHSA-2011:1458
REDHAT	RHSA-2011:1459
REDHAT	RHSA-2011:1496
URL	https://kb.isc.org/article/AA-00544/0
URL	https://kb.isc.org/article/AA-00544/74/CVE-2011-4313%3A-BIND-9-Resolver-crashes-after-logging-an-error-in-query.c.html
XF	71332

Vulnerability Solution:

- Upgrade ISC BIND to latest version

More information about upgrading your version of ISC BIND is available on the [ISC website](#).

- Apply patch to mitigate BIND 9 resolver crash

Patches mitigating this issue are available at:

- <https://www.isc.org/software/bind/981-p1>
- <https://www.isc.org/software/bind/974-p1>
- <https://www.isc.org/software/bind/96-esv-r5-p1>
- <https://www.isc.org/software/bind/94-esv-r5-p1>

3.2.88. CVE-2012-1033: Ghost Domain Names: Revoked Yet Still Resolvable (dns-bind-cve-2012-1033)*Description:*

The resolver in ISC BIND 9 through 9.8.1-P1 overwrites cached server names and TTL values in NS records during the processing of a response to an A record query, which allows remote attackers to trigger continued resolvability of revoked domain names via a "ghost domain names" attack.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2

References:

Source	Reference
BID	51898
CERT-VN	542123
CVE	CVE-2012-1033
DISA_SEVERITY	Category I
DISA_VMSKEY	V0035032
IAVM	2012-A-0189
OSVDB	78916
URL	https://kb.isc.org/article/AA-00691/74/CVE-2012-1033%3A-Ghost-Domain-Names%3A-Revoked-Yet-Still-Resolvable.html
XF	73053

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the [ISC website](#).

3.2.89. Nameserver Processes Recursive Queries (dns-processes-recursive-queries)*Description:*

Allowing nameservers to process recursive queries coming from any system may, in certain situations, help attackers conduct denial of service or cache poisoning attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:53	Nameserver resolved www.google.com to:www.google.com. 300 IN A 74.125.226.113www.google.com. 300 IN A 74.125.226.115www.google.com. 300 IN A 74.125.226.112www.google.com. 300 IN A 74.125.226.116www.google.com. 300 IN A 74.125.226.114
192.168.0.102:53	Nameserver resolved www.google.com to:www.google.com. 300 IN A 74.125.226.113www.google.com. 300 IN A 74.125.226.115www.google.com. 300 IN A 74.125.226.112www.google.com. 300 IN A 74.125.226.116www.google.com. 300 IN A 74.125.226.114

References:

Source	Reference
URL	http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf

Vulnerability Solution:

Restrict the processing of recursive queries to only systems that should be allowed to use this nameserver.

3.2.90. Debian Linux httpd Vulnerability (http-apache-0007)

Description:

The Debian GNU/Linux 2.1 Apache package by default allows anyone to view /usr/doc via the web, remotely. This is because srm.conf is preconfigured with the line:

Alias /doc/ /usr/doc/

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP service Product HTTPD exists -- Apache HTTPD 2.2.8 HTTP GET request to http://192.168.0.102/doc/ HTTP response code was an expected 200 4: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"> 5: <html> 6: <head> 4: <title>Index of /doc</title>

References:

Source	Reference
BID	318
CVE	CVE-1999-0678
URL	http://www.netSPACE.org/cgi-bin/wa?A2=ind9904a&L=bugtraq&F=&S=&P=2822

Vulnerability Solution:

The following addition to /etc/apache/access.conf will restrict access:

```
<Directory /usr/doc>
  AllowOverride None order deny,allow
  deny from all
  allow from localhost
</Directory>
```

3.2.91. PHP Multiple Vulnerabilities Fixed in version 5.2.9 (http-php-multiple-vulns-5-2-9)

Description:

The php_zip_make_relative_path function in php_zip.c in PHP 5.2.x before 5.2.9 allows context-dependent attackers to cause a denial of service (crash) via a ZIP file that contains filenames with relative paths, which is not properly handled during extraction.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-09-10-2
CVE	CVE-2009-1271
CVE	CVE-2009-1272
DEBIAN	DSA-1775
DEBIAN	DSA-1789
REDHAT	RHSA-2009:0350
URL	http://www.php.net/ChangeLog-5.php#5.2.9
URL	http://www.php.net/releases/5_2_9.php

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.9.tar.gz>

3.2.92. PHP Multiple Vulnerabilities Fixed in version 5.3.2 (http-php-multiple-vulns-5-3-2)*Description:*

Improved LCG entropy.

Fixed safe_mode validation inside tempnam() when the directory path does not end with a /.

Fixed a possible open_basedir/safe_mode bypass in the session extension identified by Grzegorz Stachowiak.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
URL	http://www.php.net/ChangeLog-5.php#5.3.2
URL	http://www.php.net/releases/5_3_2.php

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.2.tar.gz>

3.2.93. PHP Fixed security issues (CVE-2008-2665) (http-php-safemode-bypass3)*Description:*

Directory traversal vulnerability in the posix_access function in PHP 5.2.6 and earlier allows remote attackers to bypass safe_mode restrictions via a .. (dot dot) in an http URL, which results in the URL being canonicalized to a local filename after the safe_mode check has successfully run.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP service Product HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-05-12
BID	29797
CERT	TA09-133A
CVE	CVE-2008-2665
XF	43196

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.7.tar.gz>

3.2.94. No password for Grub (linux-grub-missing-passwd)*Description:*

GRUB bootloader is not password protected. An attacker can use the GRUB editor interface to change its configuration or to gather information using the cat command. It can also be exploited to boot into single user mode as root or boot into an insecure operating system.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	GRUB password not enabled in /boot/grub/menu.lst

References:

None

Vulnerability Solution:

Set a password in the GRUB configuration file. This is often located in one of several locations, but can really be anywhere:

```
/etc/grub.conf  
/boot/grub/grub.conf  
/boot/grub/menu.lst
```

To set a plain-text password, edit your GRUB configuration file and add the following line before the first uncommented line:

```
password <password>
```

To set an encrypted password, run grub-md5-crypt and use its output when adding the following line before the first uncommented line:

```
password --md5 <encryptedpassword>
```

For either approach, choose an appropriately strong password.

3.2.95. Exported volume is publicly mountable (nfs-mountd-0002)

Description:

An NFS volume is mountable by everyone. Although this is not necessarily a vulnerability itself, this does not exhibit "best practice" from a security standpoint; mounting privileges should be restricted only to hosts that require them.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:34478	/
192.168.0.102:39883	/

References:

None

Vulnerability Solution:

Restrict mounting privileges to only hosts that require them.

3.2.96. Oracle MySQL Vulnerability: CVE-2010-3833 (oracle-mysql-cve-2010-3833)

Description:

MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 does not properly propagate type errors, which allows remote attackers to cause a denial of service (server crash) via crafted arguments to extreme-value functions such as (1) LEAST and (2) GREATEST, related to KILL_BAD_DATA and a "CREATE TABLE ... SELECT."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a

Affected Nodes:	Additional Information:
	Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
APPLE	APPLE-SA-2011-06-23-1
BID	43676
CVE	CVE-2010-3833
DEBIAN	DSA-2143
REDHAT	RHSA-2010:0825
REDHAT	RHSA-2011:0164
XF	64845

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.92

Upgrade to Oracle MySQL version 5.0.92

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.51

Upgrade to Oracle MySQL version 5.1.51

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.5 and < 5.5.6

Upgrade to Oracle MySQL version 5.5.6

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.97. Oracle MySQL Vulnerability: CVE-2011-2262 (oracle-mysql-cve-2011-2262)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote attackers to affect availability via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2011-2262
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.98. Oracle MySQL Vulnerability: CVE-2012-0116 (oracle-mysql-cve-2012-0116)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect confidentiality and integrity via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0116
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.99. Oracle MySQL Vulnerability: CVE-2012-0118 (oracle-mysql-cve-2012-0118)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect confidentiality and availability via unknown vectors, a different vulnerability than CVE-2012-0113.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0118
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.100. Oracle MySQL Vulnerability: CVE-2012-0486 (oracle-mysql-cve-2012-0486)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0491, CVE-2012-0493, and CVE-2012-0495.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
BID	51514
CVE	CVE-2012-0486
OSVDB	78384
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72527

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.101. PHP Vulnerability: CVE-2007-4783 (php-cve-2007-4783)*Description:*

The iconv_substr function in PHP 5.2.4 and earlier allows context-dependent attackers to cause (1) a denial of service (application crash) via a long string in the charset parameter, probably also requiring a long string in the str parameter; or (2) a denial of service (temporary application hang) via a long string in the str parameter. NOTE: this might not be a vulnerability in most web server environments that support multiple threads, unless these issues can be demonstrated for code execution.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2007-4783
OSVDB	38917

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.5.tar.gz>

3.2.102. PHP Vulnerability: CVE-2007-4840 (php-cve-2007-4840)

Description:

PHP 5.2.4 and earlier allows context-dependent attackers to cause a denial of service (application crash) via (1) a long string in the out_charset parameter to the iconv function; or a long string in the charset parameter to the (2) iconv_mime_decode_headers, (3) iconv_mime_decode, or (4) iconv_strlen function. NOTE: this might not be a vulnerability in most web server environments that support multiple threads, unless these issues can be demonstrated for code execution.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2007-4840
OSVDB	38916
SUSE	SUSE-SA:2008:004

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.5.tar.gz>

3.2.103. PHP Vulnerability: CVE-2008-2666 (php-cve-2008-2666)

Description:

Multiple directory traversal vulnerabilities in PHP 5.2.6 and earlier allow context-dependent attackers to bypass safe_mode restrictions by creating a subdirectory named http: and then placing ../ (dot dot slash) sequences in an http URL argument to the (1) chdir or (2) ftok function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-05-12

Source	Reference
BID	29796
CERT	TA09-133A
CVE	CVE-2008-2666
XF	43198

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.7.tar.gz>

3.2.104. PHP Vulnerability: CVE-2008-4107 (php-cve-2008-4107)*Description:*

The (1) rand and (2) mt_rand functions in PHP 5.2.6 do not produce cryptographically strong random numbers, which allows attackers to leverage exposures in products that rely on these functions for security-relevant functionality, as demonstrated by the password-reset functionality in Joomla! 1.5.x and WordPress before 2.6.2, a different vulnerability than CVE-2008-2107, CVE-2008-2108, and CVE-2008-4102.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
BID	31115
CVE	CVE-2008-4107
OSVDB	48700
XF	45956

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.6.tar.gz>

3.2.105. PHP Vulnerability: CVE-2008-5498 (php-cve-2008-5498)*Description:*

Array index error in the imageRotate function in PHP 5.2.8 and earlier allows context-dependent attackers to read the contents of arbitrary memory locations via a crafted value of the third argument (aka the bgd_color or clrBack argument) for an indexed image.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-09-10-2
BID	33002
CVE	CVE-2008-5498
OSVDB	51031
OVAL	OVAL9667
REDHAT	RHSA-2009:0350
XF	47635

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.9.tar.gz>

3.2.106. PHP Vulnerability: CVE-2009-1272 (php-cve-2009-1272)*Description:*

The `php_zip_make_relative_path` function in `php_zip.c` in PHP 5.2.x before 5.2.9 allows context-dependent attackers to cause a denial of service (crash) via a ZIP file that contains filenames with relative paths, which is not properly handled during extraction.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-09-10-2
CVE	CVE-2009-1272
URL	http://www.php.net/releases/5_2_9.php

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.9.tar.gz>

3.2.107. PHP Vulnerability: CVE-2009-4418 (php-cve-2009-4418)

Description:

The unserialize function in PHP 5.3.0 and earlier allows context-dependent attackers to cause a denial of service (resource consumption) via a deeply nested serialized variable, as demonstrated by a string beginning with a:1: followed by many {a:1: sequences.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2009-4418

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.1.tar.gz>

3.2.108. PHP Vulnerability: CVE-2010-1860 (php-cve-2010-1860)

Description:

The html_entity_decode function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal call, related to the call time pass by reference feature.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2010-1860

Vulnerability Solution:

- Upgrade to PHP version 5.2.14

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.14.tar.gz>

•Upgrade to PHP version 5.3.3

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.3.tar.gz>

3.2.109. PHP Vulnerability: CVE-2010-1862 (php-cve-2010-1862)

Description:

The chunk_split function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2010-1862

Vulnerability Solution:

•Upgrade to PHP version 5.2.14

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.14.tar.gz>

•Upgrade to PHP version 5.3.3

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.3.tar.gz>

3.2.110. PHP Vulnerability: CVE-2010-1864 (php-cve-2010-1864)

Description:

The addslashes function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2010-1864

Vulnerability Solution:

- Upgrade to PHP version 5.2.14

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.14.tar.gz>

- Upgrade to PHP version 5.3.3

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.3.tar.gz>

3.2.111. PHP Vulnerability: CVE-2010-1915 (php-cve-2010-1915)*Description:*

The preg_quote function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature, modification of ZVALs whose values are not updated in the associated local variables, and access of previously-freed memory.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2010-1915
XF	58586

Vulnerability Solution:

- Upgrade to PHP version 5.2.14

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.14.tar.gz>

- Upgrade to PHP version 5.3.3

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.3.tar.gz>

3.2.112. PHP Vulnerability: CVE-2010-2093 (php-cve-2010-2093)*Description:*

Use-after-free vulnerability in the request shutdown functionality in PHP 5.2 before 5.2.13 and 5.3 before 5.3.2 allows context-dependent attackers to cause a denial of service (crash) via a stream context structure that is freed before destruction occurs.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2010-2093

Vulnerability Solution:

- Upgrade to PHP version 5.2.14

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.14.tar.gz>

- Upgrade to PHP version 5.3.3

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.3.tar.gz>

3.2.113. PHP Vulnerability: CVE-2010-2097 (php-cve-2010-2097)*Description:*

The (1) iconv_mime_decode, (2) iconv_substr, and (3) iconv_mime_encode functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2010-2097

Vulnerability Solution:

- Upgrade to PHP version 5.2.14

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.14.tar.gz>

- Upgrade to PHP version 5.3.3

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.3.tar.gz>

3.2.114. PHP Vulnerability: CVE-2010-2100 (php-cve-2010-2100)

Description:

The (1) htmlentities, (2) htmlspecialchars, (3) str_getcsv, (4) http_build_query, (5) strpbrk, and (6) strstr functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2010-2100

Vulnerability Solution:

- Upgrade to PHP version 5.2.14

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.14.tar.gz>

- Upgrade to PHP version 5.3.3

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.3.tar.gz>

3.2.115. PHP Vulnerability: CVE-2010-2101 (php-cve-2010-2101)*Description:*

The (1) strip_tags, (2) setcookie, (3) strtok, (4) wordwrap, (5) str_word_count, and (6) str_pad functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2010-2101

Vulnerability Solution:

- Upgrade to PHP version 5.2.14

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.14.tar.gz>

- Upgrade to PHP version 5.3.3

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.3.tar.gz>

3.2.116. PHP Vulnerability: CVE-2010-2190 (php-cve-2010-2190)

Description:

The (1) trim, (2) ltrim, (3) rtrim, and (4) substr_replace functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2010-2190
XF	59220

Vulnerability Solution:

- Upgrade to PHP version 5.2.14

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.14.tar.gz>

- Upgrade to PHP version 5.3.3

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.3.tar.gz>

3.2.117. PHP Vulnerability: CVE-2010-4150 (php-cve-2010-4150)

Description:

Double free vulnerability in the imap_do_open function in the IMAP extension (ext/imap/php_imap.c) in PHP 5.2 before 5.2.15 and 5.3 before 5.3.4 allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
BID	44980
CVE	CVE-2010-4150
OVAL	OVAL12489
XF	63390

Vulnerability Solution:

- Upgrade to PHP version 5.2.15

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.15.tar.gz>

- Upgrade to PHP version 5.3.4

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.4.tar.gz>

3.2.118. PHP Vulnerability: CVE-2010-4699 (php-cve-2010-4699)*Description:*

The `iconv_mime_decode_headers` function in the `Iconv` extension in PHP before 5.3.4 does not properly handle encodings that are unrecognized by the `iconv` and `mbstring` (aka Multibyte String) implementations, which allows remote attackers to trigger an incomplete output array, and possibly bypass spam detection or have unspecified other impact, via a crafted Subject header in an e-mail message, as demonstrated by the `ks_c_5601-1987` character set.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2010-4699
OVAL	OVAL12393
XF	64963

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.4.tar.gz>

3.2.119. PHP Vulnerability: CVE-2011-0752 (php-cve-2011-0752)

Description:

The extract function in PHP before 5.2.15 does not prevent use of the EXTR_OVERWRITE parameter to overwrite (1) the GLOBALS superglobal array and (2) the this variable, which allows context-dependent attackers to bypass intended access restrictions by modifying data structures that were not intended to depend on external input, a related issue to CVE-2005-2691 and CVE-2006-3758.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2011-0752
OVAL	OVAL12016
XF	65432

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.15.tar.gz>

3.2.120. PHP Vulnerability: CVE-2011-0755 (php-cve-2011-0755)*Description:*

Integer overflow in the mt_rand function in PHP before 5.3.4 might make it easier for context-dependent attackers to predict the return values by leveraging a script's use of a large max parameter, as demonstrated by a value that exceeds mt_getrandmax.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2011-0755
OVAL	OVAL12589
XF	65426

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.4.tar.gz>

3.2.121. PHP Vulnerability: CVE-2012-0789 (php-cve-2012-0789)

Description:

Memory leak in the timezone functionality in PHP before 5.3.9 allows remote attackers to cause a denial of service (memory consumption) by triggering many strtotime function calls, which are not properly handled by the php_date_parse_tzfile cache.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2012-0789

Vulnerability Solution:

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.122. PHP Vulnerability: CVE-2012-1171 (php-cve-2012-1171)

Description:

The libxml RSHUTDOWN function in PHP 5.x allows remote attackers to bypass the open_basedir protection mechanism and read arbitrary files via vectors involving a stream_close method call during use of a custom stream wrapper.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2012-1171

Vulnerability Solution:

- Upgrade to PHP version 5.3.28

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 5.4.24

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 5.5.7

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.123. PHP Vulnerability: CVE-2012-2336 (php-cve-2012-2336)

Description:

sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to cause a denial of service (resource consumption) by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'T' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2012-2336
URL	http://www.php.net/archive/2012.php#id2012-05-08-1
URL	https://bugs.php.net/bug.php?id=61910

Vulnerability Solution:

- Upgrade to PHP version 5.3.13

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 5.4.3

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.124. PHP Vulnerability: CVE-2012-3365 (php-cve-2012-3365)

Description:

The SQLite functionality in PHP before 5.3.15 allows remote attackers to bypass the open_basedir protection mechanism via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2012-3365

Vulnerability Solution:

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.125. PHP Vulnerability: CVE-2013-1643 (php-cve-2013-1643)*Description:*

The SOAP parser in PHP before 5.3.23 and 5.4.x before 5.4.13 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-1824.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CVE	CVE-2013-1643
DEBIAN	DSA-2639
REDHAT	RHSA-2013:1307
REDHAT	RHSA-2013:1615

Vulnerability Solution:

- Upgrade to PHP version 5.3.23

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 5.4.13

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.126. PHP Vulnerability: CVE-2013-2110 (php-cve-2013-2110)

Description:

Heap-based buffer overflow in the `php_quot_print_encode` function in `ext/standard/quot_print.c` in PHP before 5.3.26 and 5.4.x before 5.4.16 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted argument to the `quoted_printable_encode` function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
CVE	CVE-2013-2110

Vulnerability Solution:

- Upgrade to PHP version 5.3.26
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.4.16
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.127. PHP Vulnerability: CVE-2013-6501 (php-cve-2013-6501)*Description:*

The default `soap.wsdl_cache_dir` setting in (1) `php.ini-production` and (2) `php.ini-development` in PHP through 5.6.7 specifies the `/tmp` directory, which makes it easier for local users to conduct WSDL injection attacks by creating a file under `/tmp` with a predictable filename that is used by the `get_sdl` function in `ext/soap/php_sdl.c`.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2013-6501

Vulnerability Solution:

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.128. PHP Vulnerability: CVE-2014-9652 (php-cve-2014-9652)*Description:*

The mconvert function in softmagic.c in file before 5.21, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not properly handle a certain string-length field during a copy of a truncated version of a Pascal string, which might allow remote attackers to cause a denial of service (out-of-bounds memory access and application crash) via a crafted file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2014-9652

Vulnerability Solution:

- Upgrade to PHP version 5.4.37

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 5.5.21

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 5.6.5

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.129. PHP Vulnerability: CVE-2014-9709 (php-cve-2014-9709)*Description:*

The GetCode_ function in gd_gif_in.c in GD 2.1.1 and earlier, as used in PHP before 5.5.21 and 5.6.x before 5.6.5, allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted GIF image that is improperly handled by the gdImageCreateFromGif function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2014-9709
DEBIAN	DSA-3215

Vulnerability Solution:

- Upgrade to PHP version 5.4.38
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.5.22
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.6.6
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.130. PHP Vulnerability: CVE-2015-1352 (php-cve-2015-1352)*Description:*

The build_tablename function in pgsql.c in the PostgreSQL (aka postgres) extension in PHP through 5.6.7 does not validate token extraction for table names, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted name.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2015-1352

Vulnerability Solution:

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.131. PHP Vulnerability: CVE-2015-2348 (php-cve-2015-2348)*Description:*

The move_uploaded_file implementation in ext/standard/basic_functions.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 truncates a pathname upon encountering a \x00 character, which allows remote attackers to bypass intended extension restrictions and create files with unexpected names via a crafted second argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2015-2348

Vulnerability Solution:

- Upgrade to PHP version 5.4.39
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.5.23
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 5.6.7
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.132. PHP Fixed iconv_*() functions to limit argument sizes (CVE-2007-4783) (php-fixed-iconv-functions-to-limit-argument-sizes-cve-2007-4783)

Description:

The iconv_substr function in PHP 5.2.4 and earlier allows context-dependent attackers to cause (1) a denial of service (application crash) via a long string in the charset parameter, probably also requiring a long string in the str parameter; or (2) a denial of service (temporary application hang) via a long string in the str parameter. NOTE: this might not be a vulnerability in most web server environments that support multiple threads, unless these issues can be demonstrated for code execution.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2007-4783
OSVDB	38917

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.5.tar.gz>

3.2.133. PHP Fixed iconv_*() functions to limit argument sizes (CVE-2007-4840) (php-fixed-iconv-functions-to-limit-argument-sizes-cve-2007-4840)

Description:

PHP 5.2.4 and earlier allows context-dependent attackers to cause a denial of service (application crash) via (1) a long string in the out_charset parameter to the iconv function; or a long string in the charset parameter to the (2) iconv_mime_decode_headers, (3) iconv_mime_decode, or (4) iconv_strlen function. NOTE: this might not be a vulnerability in most web server environments that support multiple threads, unless these issues can be demonstrated for code execution.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2007-4840
OSVDB	38916
SUSE	SUSE-SA:2008:004

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.5.tar.gz>

3.2.134. PHP Fixed security issue in imagerotate() (php-fixed-security-issue-in-imagerotate)

Description:

Array index error in the imageRotate function in PHP 5.2.8 and earlier allows context-dependent attackers to read the contents of arbitrary memory locations via a crafted value of the third argument (aka the bgd_color or clrBack argument) for an indexed image.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference

Source	Reference
APPLE	APPLE-SA-2009-09-10-2
BID	33002
CVE	CVE-2008-5498
OSVDB	51031
OVAL	OVAL9667
REDHAT	RHSA-2009:0350
XF	47635

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.9.tar.gz>

3.2.135. PHP Fixed security issues (CVE-2008-2666) (php-fixed-security-issues-cve-2008-2666)*Description:*

Multiple directory traversal vulnerabilities in PHP 5.2.6 and earlier allow context-dependent attackers to bypass safe_mode restrictions by creating a subdirectory named http: and then placing ../ (dot dot slash) sequences in an http URL argument to the (1) chdir or (2) ftok function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-05-12
BID	29796
CERT	TA09-133A
CVE	CVE-2008-2666
XF	43198

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.7.tar.gz>

3.2.136. PHP possible double free in imap extension (php-possible-double-free-in-imag-extension)*Description:*

Double free vulnerability in the `imap_do_open` function in the IMAP extension (`ext/imap/php_imap.c`) in PHP 5.2 before 5.2.15 and 5.3 before 5.3.4 allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
BID	44980
CVE	CVE-2010-4150
OVAL	OVAL12489
XF	63390

Vulnerability Solution:

- Upgrade to PHP version 5.2.15

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.15.tar.gz>

- Upgrade to PHP version 5.3.4

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.4.tar.gz>

3.2.137. TCP Sequence Number Approximation Vulnerability (`tcp-seq-num-approximation`)

Description:

TCP, when using a large Window Size, makes it easier for remote attackers to guess sequence numbers and cause a denial of service (connection loss) to persistent TCP connections by repeatedly injecting a TCP RST packet, especially in protocols that use long-lived connections, such as BGP.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	TCP reset with incorrect sequence number triggered this fault: Connection reset by peer

References:

Source	Reference

Source	Reference
BID	10183
CERT	TA04-111A
CERT-VN	415294
CVE	CVE-2004-0230
MS	MS05-019
MS	MS06-064
NETBSD	NetBSD-SA2004-006
OSVDB	4030
OVAL	OVAL2689
OVAL	OVAL270
OVAL	OVAL3508
OVAL	OVAL4791
OVAL	OVAL5711
SGI	20040403-01-A
URL	ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc
URL	http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12
URL	http://www.uniras.gov.uk/vuls/2004/236929/index.htm
XF	15886

Vulnerability Solution:

- Enable TCP MD5 Signatures

Enable the TCP MD5 signature option as documented in [RFC 2385](#). It was designed to reduce the danger from certain security attacks on BGP, such as TCP resets.

- Microsoft Windows 2000 SP4 OR SP3 (x86), Microsoft Windows 2000 Professional SP4 OR SP3 (x86), Microsoft Windows 2000 Server SP4 OR SP3 (x86), Microsoft Windows 2000 Advanced Server SP4 OR SP3 (x86), Microsoft Windows 2000 Datacenter Server SP4 OR SP3 (x86)

MS05-019: Security Update for Windows 2000 (KB893066)

Download and apply the patch from: <http://go.microsoft.com/fwlink/?LinkId=36661>

- Microsoft Windows Server 2003 < SP1 (x86), Microsoft Windows Server 2003, Standard Edition < SP1 (x86), Microsoft Windows Server 2003, Enterprise Edition < SP1 (x86), Microsoft Windows Server 2003, Datacenter Edition < SP1 (x86), Microsoft Windows Server 2003, Web Edition < SP1 (x86), Microsoft Windows Small Business Server 2003 < SP1 (x86)

MS05-019: Security Update for Windows Server 2003 (KB893066)

Download and apply the patch from: <http://go.microsoft.com/fwlink/?LinkId=36661>

- Microsoft Windows XP Professional SP2 OR SP1 (x86), Microsoft Windows XP Home SP2 OR SP1 (x86)

MS05-019: Security Update for Windows XP (KB893066)

Download and apply the patch from: <http://go.microsoft.com/fwlink/?LinkId=36661>

- Microsoft Windows XP Professional SP1 OR SP2 (x86), Microsoft Windows XP Home SP1 OR SP2 (x86)

MS06-064: Security Update for Windows XP (KB922819)

Download and apply the patch from: <http://go.microsoft.com/fwlink/?LinkId=73864>

- Microsoft Windows Server 2003 SP1 (x86_64), Microsoft Windows Server 2003, Standard Edition SP1 (x86_64), Microsoft Windows Server 2003, Enterprise Edition SP1 (x86_64), Microsoft Windows Server 2003, Datacenter Edition SP1 (x86_64), Microsoft Windows Server 2003, Web Edition SP1 (x86_64), Microsoft Windows Small Business Server 2003 SP1 (x86_64)

MS06-064: Security Update for Windows Server 2003 x64 Edition (KB922819)

Download and apply the patch from: <http://go.microsoft.com/fwlink/?LinkId=73864>

- Microsoft Windows XP Professional SP1 (x86_64)

MS06-064: Security Update for Windows XP x64 Edition (KB922819)

Download and apply the patch from: <http://go.microsoft.com/fwlink/?LinkId=73864>

- Microsoft Windows Server 2003 SP1 OR < SP1 (ia64), Microsoft Windows Server 2003, Standard Edition SP1 OR < SP1 (ia64), Microsoft Windows Server 2003, Enterprise Edition SP1 OR < SP1 (ia64), Microsoft Windows Server 2003, Datacenter Edition SP1 OR < SP1 (ia64), Microsoft Windows Server 2003, Web Edition SP1 OR < SP1 (ia64), Microsoft Windows Small Business Server 2003 SP1 OR < SP1 (ia64)

MS06-064: Security Update for Windows Server 2003 for Itanium-based Systems (KB922819)

Download and apply the patch from: <http://go.microsoft.com/fwlink/?LinkId=73864>

- Microsoft Windows Server 2003 SP1 OR < SP1 (x86), Microsoft Windows Server 2003, Standard Edition SP1 OR < SP1 (x86), Microsoft Windows Server 2003, Enterprise Edition SP1 OR < SP1 (x86), Microsoft Windows Server 2003, Datacenter Edition SP1 OR < SP1 (x86), Microsoft Windows Server 2003, Web Edition SP1 OR < SP1 (x86), Microsoft Windows Small Business Server 2003 SP1 OR < SP1 (x86)

MS06-064: Security Update for Windows Server 2003 (KB922819)

Download and apply the patch from: <http://go.microsoft.com/fwlink/?LinkId=73864>

- Locate and fix vulnerable traffic inspection devices along the route to the target

In many situations, target systems are, by themselves, patched or otherwise unaffected by this vulnerability. In certain configurations, however, unaffected systems can be made vulnerable if the path between an attacker and the target system contains an affected and unpatched network device such as a firewall or router and that device is responsible for handling TCP connections for the target. In this case, locate and apply remediation steps for network devices along the route that are affected.

3.2.138. USN-1017-1: MySQL vulnerabilities (ubuntu-usn-1017-1)

Description:

MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 does not properly propagate type errors, which allows remote attackers to cause a denial of service (server crash) via crafted arguments to extreme-value functions such as (1) LEAST and (2) GREATEST, related to KILL_BAD_DATA and a "CREATE TABLE ... SELECT."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04

Affected Nodes:	Additional Information:
	Vulnerable software installed: Ubuntu mysql-server-5.0 5.0.51a-3ubuntu5

References:

Source	Reference
APPLE	APPLE-SA-2011-06-23-1
BID	41198
BID	42596
BID	42598
BID	42599
BID	42625
BID	42633
BID	42638
BID	42646
BID	43676
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
DEBIAN	DSA-2143
OVAL	OVAL11869
REDHAT	RHSA-2010:0824

Source	Reference
REDHAT	RHSA-2010:0825
REDHAT	RHSA-2011:0164
USN	USN-1017-1
XF	64683
XF	64684
XF	64685
XF	64686
XF	64687
XF	64688
XF	64838
XF	64839
XF	64840
XF	64841
XF	64842
XF	64843
XF	64844
XF	64845

Vulnerability Solution:

- mysql-server-5.0 on Ubuntu Linux 8.04
Upgrade mysql-server-5.0 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade mysql-server-5.0 to the latest version
- mysql-server-5.1 on Ubuntu Linux 10.04
Upgrade mysql-server-5.1 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade mysql-server-5.1 to the latest version
- mysql-server-5.1 on Ubuntu Linux 10.10
Upgrade mysql-server-5.1 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade mysql-server-5.1 to the latest version
- mysql-server-5.1 on Ubuntu Linux 9.10
Upgrade mysql-server-5.1 for Ubuntu 9.10
Use `apt-get upgrade` to upgrade mysql-server-5.1 to the latest version

3.2.139. USN-1021-1: Apache vulnerabilities (ubuntu-usn-1021-1)

Description:

Memory leak in the `apr_brigade_split_line` function in `buckets/apr_brigade.c` in the Apache Portable Runtime Utility library (aka APR-util) before 1.3.10, as used in the `mod_reqtimeout` module in the Apache HTTP Server and other software, allows remote attackers to

cause a denial of service (memory consumption) via unspecified vectors related to the destruction of an APR bucket.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu apache2.2-common 2.2.8-1ubuntu0.15

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
BID	43673
CVE	CVE-2010-1452
CVE	CVE-2010-1623
OVAL	OVAL11683
OVAL	OVAL12341
OVAL	OVAL12800
REDHAT	RHSA-2010:0659
REDHAT	RHSA-2010:0950
REDHAT	RHSA-2011:0896
REDHAT	RHSA-2011:0897
USN	USN-1021-1

Vulnerability Solution:

- apache2.2-common on Ubuntu Linux 10.04
Upgrade apache2.2-common for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade apache2.2-common to the latest version
- apache2.2-common on Ubuntu Linux 10.10
Upgrade apache2.2-common for Ubuntu 10.10
Use `apt-get upgrade` to upgrade apache2.2-common to the latest version
- apache2.2-common on Ubuntu Linux 8.04
Upgrade apache2.2-common for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade apache2.2-common to the latest version
- apache2.2-common on Ubuntu Linux 9.10
Upgrade apache2.2-common for Ubuntu 9.10
Use `apt-get upgrade` to upgrade apache2.2-common to the latest version

3.2.140. USN-1022-1: APR-util vulnerability (ubuntu-usn-1022-1)*Description:*

Memory leak in the `apr_brigade_split_line` function in `buckets/apr_brigade.c` in the Apache Portable Runtime Utility library (aka APR-util) before 1.3.10, as used in the `mod_reqtimeout` module in the Apache HTTP Server and other software, allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors related to the destruction of an APR bucket.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libaprutil1 1.2.12+dfsg-3

References:

Source	Reference
BID	43673
CVE	CVE-2010-1623
OVAL	OVAL12800
REDHAT	RHSA-2010:0950
REDHAT	RHSA-2011:0896
REDHAT	RHSA-2011:0897
USN	USN-1022-1

Vulnerability Solution:

- libaprutil1 on Ubuntu Linux 10.04
Upgrade libaprutil1 for Ubuntu 10.04 LTS
Use ``apt-get upgrade`` to upgrade libaprutil1 to the latest version
- libaprutil1 on Ubuntu Linux 10.10
Upgrade libaprutil1 for Ubuntu 10.10
Use ``apt-get upgrade`` to upgrade libaprutil1 to the latest version
- libaprutil1 on Ubuntu Linux 8.04
Upgrade libaprutil1 for Ubuntu 8.04 LTS
Use ``apt-get upgrade`` to upgrade libaprutil1 to the latest version
- libaprutil1 on Ubuntu Linux 9.10
Upgrade libaprutil1 for Ubuntu 9.10
Use ``apt-get upgrade`` to upgrade libaprutil1 to the latest version

3.2.141. USN-1075-1: Samba vulnerability (ubuntu-usn-1075-1)

Description:

Samba 3.x before 3.3.15, 3.4.x before 3.4.12, and 3.5.x before 3.5.7 does not perform range checks for file descriptors before use of the FD_SET macro, which allows remote attackers to cause a denial of service (stack memory corruption, and infinite loop or daemon crash) by opening a large number of files, related to (1) Winbind or (2) smbd.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu samba 3.0.20-0.1ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2011-06-23-1
BID	46597
CVE	CVE-2011-0719
DEBIAN	DSA-2175
REDHAT	RHSA-2011:0305
REDHAT	RHSA-2011:0306
USN	USN-1075-1
XF	65724

Vulnerability Solution:

- samba on Ubuntu Linux 10.04
Upgrade samba for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade samba to the latest version
- samba on Ubuntu Linux 10.10
Upgrade samba for Ubuntu 10.10
Use `apt-get upgrade` to upgrade samba to the latest version
- samba on Ubuntu Linux 8.04
Upgrade samba for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade samba to the latest version
- samba on Ubuntu Linux 9.10
Upgrade samba for Ubuntu 9.10
Use `apt-get upgrade` to upgrade samba to the latest version

3.2.142. USN-1229-1: PostgreSQL vulnerability (ubuntu-usn-1229-1)

Description:

crypt_blowfish before 1.1, as used in PHP before 5.3.7 on certain platforms, PostgreSQL before 8.4.9, and other products, does not properly handle 8-bit characters, which makes it easier for context-dependent attackers to determine a cleartext password by leveraging knowledge of a password hash.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu postgresql-8.3 8.3.1-1

References:

Source	Reference
APPLE	APPLE-SA-2012-02-01-1
BID	49241
CVE	CVE-2011-2483
DEBIAN	DSA-2340
DEBIAN	DSA-2399
REDHAT	RHSA-2011:1377
REDHAT	RHSA-2011:1378
REDHAT	RHSA-2011:1423
SUSE	SUSE-SA:2011:035
USN	USN-1229-1
XF	69319

Vulnerability Solution:

- postgresql-8.3 on Ubuntu Linux 8.04
Upgrade postgresql-8.3 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version
- postgresql-8.4 on Ubuntu Linux 10.04
Upgrade postgresql-8.4 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version
- postgresql-8.4 on Ubuntu Linux 10.10
Upgrade postgresql-8.4 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version
- postgresql-8.4 on Ubuntu Linux 11.04
Upgrade postgresql-8.4 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version

3.2.143. USN-1259-1: Apache vulnerabilities (ubuntu-usn-1259-1)*Description:*

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu apache2.2-common 2.2.8-1ubuntu0.15

References:

Source	Reference
APPLE	APPLE-SA-2012-02-01-1
APPLE	APPLE-SA-2012-09-19-2
BID	46953
BID	49616
BID	49957
CVE	CVE-2011-1176
CVE	CVE-2011-3348
CVE	CVE-2011-3368
DEBIAN	DSA-2202
OSVDB	76079
OVAL	OVAL14941
OVAL	OVAL18154
REDHAT	RHSA-2011:1391
REDHAT	RHSA-2011:1392
USN	USN-1259-1
XF	66248
XF	69804
XF	70336

Vulnerability Solution:

- apache2-mpm-itk on Ubuntu Linux 10.04
Upgrade apache2-mpm-itk for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade apache2-mpm-itk to the latest version
- apache2-mpm-itk on Ubuntu Linux 10.10
Upgrade apache2-mpm-itk for Ubuntu 10.10
Use `apt-get upgrade` to upgrade apache2-mpm-itk to the latest version
- apache2-mpm-itk on Ubuntu Linux 11.04
Upgrade apache2-mpm-itk for Ubuntu 11.04
Use `apt-get upgrade` to upgrade apache2-mpm-itk to the latest version
- apache2.2-bin on Ubuntu Linux 10.04
Upgrade apache2.2-bin for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade apache2.2-bin to the latest version
- apache2.2-bin on Ubuntu Linux 10.10
Upgrade apache2.2-bin for Ubuntu 10.10
Use `apt-get upgrade` to upgrade apache2.2-bin to the latest version
- apache2.2-bin on Ubuntu Linux 11.04
Upgrade apache2.2-bin for Ubuntu 11.04
Use `apt-get upgrade` to upgrade apache2.2-bin to the latest version
- apache2.2-bin on Ubuntu Linux 11.10
Upgrade apache2.2-bin for Ubuntu 11.10
Use `apt-get upgrade` to upgrade apache2.2-bin to the latest version
- apache2.2-common on Ubuntu Linux 8.04
Upgrade apache2.2-common for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade apache2.2-common to the latest version

3.2.144. USN-1308-1: bzip2 vulnerability (ubuntu-usn-1308-1)

Description:

The bzexe command in bzip2 1.0.5 and earlier generates compressed executables that do not properly handle temporary files during extraction, which allows local users to execute arbitrary code by precreating a temporary directory.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu bzip2 1.0.4-2ubuntu4

References:

Source	Reference

Source	Reference
CVE	CVE-2011-4089
USN	USN-1308-1

Vulnerability Solution:

•bzip2 on Ubuntu Linux 10.04

Upgrade bzip2 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade bzip2 to the latest version

•bzip2 on Ubuntu Linux 10.10

Upgrade bzip2 for Ubuntu 10.10

Use `apt-get upgrade` to upgrade bzip2 to the latest version

•bzip2 on Ubuntu Linux 11.04

Upgrade bzip2 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade bzip2 to the latest version

•bzip2 on Ubuntu Linux 11.10

Upgrade bzip2 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade bzip2 to the latest version

•bzip2 on Ubuntu Linux 8.04

Upgrade bzip2 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade bzip2 to the latest version

3.2.145. USN-1368-1: Apache HTTP Server vulnerabilities (ubuntu-usn-1368-1)*Description:*

scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu apache2.2-common 2.2.8-1ubuntu0.15

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
BID	50494
BID	51407

Source	Reference
BID	51706
CVE	CVE-2011-3607
CVE	CVE-2011-4317
CVE	CVE-2012-0021
CVE	CVE-2012-0031
CVE	CVE-2012-0053
OSVDB	76744
REDHAT	RHSA-2012:0128
USN	USN-1368-1
XF	71093

Vulnerability Solution:

- apache2.2-common on Ubuntu Linux 10.04
Upgrade apache2.2-common for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade apache2.2-common to the latest version
- apache2.2-common on Ubuntu Linux 10.10
Upgrade apache2.2-common for Ubuntu 10.10
Use `apt-get upgrade` to upgrade apache2.2-common to the latest version
- apache2.2-common on Ubuntu Linux 11.04
Upgrade apache2.2-common for Ubuntu 11.04
Use `apt-get upgrade` to upgrade apache2.2-common to the latest version
- apache2.2-common on Ubuntu Linux 11.10
Upgrade apache2.2-common for Ubuntu 11.10
Use `apt-get upgrade` to upgrade apache2.2-common to the latest version
- apache2.2-common on Ubuntu Linux 8.04
Upgrade apache2.2-common for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade apache2.2-common to the latest version

3.2.146. USN-1376-1: libxml2 vulnerability (ubuntu-usn-1376-1)*Description:*

libxml2 before 2.8.0 computes hash values without restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted XML data.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04

Affected Nodes:	Additional Information:
	Vulnerable software installed: Ubuntu libxml2 2.6.31.dfsg-2ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2013-09-18-2
APPLE	APPLE-SA-2013-10-22-8
BID	52107
CVE	CVE-2012-0841
DEBIAN	DSA-2417
DISA_SEVERITY	Category I
DISA_VMSKEY	V0033794
DISA_VMSKEY	V0033884
IAVM	2012-A-0148
IAVM	2012-A-0153
REDHAT	RHSA-2012:0324
REDHAT	RHSA-2013:0217
USN	USN-1376-1

Vulnerability Solution:

- libxml2 on Ubuntu Linux 10.04
Upgrade libxml2 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libxml2 to the latest version
- libxml2 on Ubuntu Linux 10.10
Upgrade libxml2 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libxml2 to the latest version
- libxml2 on Ubuntu Linux 11.04
Upgrade libxml2 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade libxml2 to the latest version
- libxml2 on Ubuntu Linux 11.10
Upgrade libxml2 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade libxml2 to the latest version
- libxml2 on Ubuntu Linux 8.04
Upgrade libxml2 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libxml2 to the latest version

3.2.147. USN-1418-1: GnuTLS vulnerabilities (ubuntu-usn-1418-1)

Description:

gnutls_cipher.c in libgnutls in GnuTLS before 2.12.17 and 3.x before 3.0.15 does not properly handle data encrypted with a block cipher, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) via a crafted record, as demonstrated by a crafted GenericBlockCipher structure.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libgnutls13 2.0.4-1ubuntu2

References:

Source	Reference
CVE	CVE-2011-4128
CVE	CVE-2012-1573
DISA_SEVERITY	Category I
DISA_VMSKEY	V0033794
DISA_VMSKEY	V0033884
IAVM	2012-A-0148
IAVM	2012-A-0153
OSVDB	80259
REDHAT	RHSA-2012:0429
REDHAT	RHSA-2012:0488
REDHAT	RHSA-2012:0531
USN	USN-1418-1

Vulnerability Solution:

•libgnutls13 on Ubuntu Linux 8.04

Upgrade libgnutls13 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libgnutls13 to the latest version

•libgnutls26 on Ubuntu Linux 10.04

Upgrade libgnutls26 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libgnutls26 to the latest version

•libgnutls26 on Ubuntu Linux 10.10

Upgrade libgnutls26 for Ubuntu 10.10

Use `apt-get upgrade` to upgrade libgnutls26 to the latest version

- libgnutls26 on Ubuntu Linux 11.04

Upgrade libgnutls26 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libgnutls26 to the latest version

- libgnutls26 on Ubuntu Linux 11.10

Upgrade libgnutls26 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libgnutls26 to the latest version

3.2.148. USN-1436-1: Libtasn1 vulnerability (ubuntu-usn-1436-1)

Description:

The `asn1_get_length_der` function in `decoding.c` in GNU Libtasn1 before 2.12, as used in GnuTLS before 3.0.16 and other products, does not properly handle certain large length values, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly have unspecified other impact via a crafted ASN.1 structure.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libtasn1-3 1.1-1

References:

Source	Reference
CVE	CVE-2012-1569
DISA_SEVERITY	Category I
DISA_VMSKEY	V0033794
DISA_VMSKEY	V0033884
IAVM	2012-A-0148
IAVM	2012-A-0153
REDHAT	RHSA-2012:0488
REDHAT	RHSA-2012:0531
USN	USN-1436-1

Vulnerability Solution:

- libtasn1-3 on Ubuntu Linux 10.04

Upgrade libtasn1-3 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libtasn1-3 to the latest version

- libtasn1-3 on Ubuntu Linux 11.04

Upgrade libtasn1-3 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libtasn1-3 to the latest version

- libtasn1-3 on Ubuntu Linux 11.10

Upgrade libtasn1-3 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libtasn1-3 to the latest version

- libtasn1-3 on Ubuntu Linux 12.04

Upgrade libtasn1-3 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libtasn1-3 to the latest version

- libtasn1-3 on Ubuntu Linux 8.04

Upgrade libtasn1-3 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libtasn1-3 to the latest version

3.2.149. USN-1467-1: MySQL vulnerabilities (ubuntu-usn-1467-1)

Description:

sql/password.c in Oracle MySQL 5.1.x before 5.1.63, 5.5.x before 5.5.24, and 5.6.x before 5.6.6, and MariaDB 5.1.x before 5.1.62, 5.2.x before 5.2.12, 5.3.x before 5.3.6, and 5.5.x before 5.5.23, when running in certain environments with certain implementations of the memcmp function, allows remote attackers to bypass authentication by repeatedly authenticating with the same incorrect password, which eventually causes a token comparison to succeed due to an improperly-checked return value.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu mysql-server-5.0 5.0.51a-3ubuntu5

References:

Source	Reference
BID	53911
CVE	CVE-2012-2122
USN	USN-1467-1

Vulnerability Solution:

- mysql-server-5.0 on Ubuntu Linux 8.04

Upgrade mysql-server-5.0 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade mysql-server-5.0 to the latest version

- mysql-server-5.1 on Ubuntu Linux 10.04

Upgrade mysql-server-5.1 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade mysql-server-5.1 to the latest version

- mysql-server-5.1 on Ubuntu Linux 11.04

Upgrade mysql-server-5.1 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade mysql-server-5.1 to the latest version

- mysql-server-5.1 on Ubuntu Linux 11.10

Upgrade mysql-server-5.1 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade mysql-server-5.1 to the latest version

- mysql-server-5.5 on Ubuntu Linux 12.04

Upgrade mysql-server-5.5 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade mysql-server-5.5 to the latest version

3.2.150. USN-1527-1: Expat vulnerabilities (ubuntu-usn-1527-1)

Description:

Memory leak in the poolGrow function in expat/lib/xmlparse.c in expat before 2.1.0 allows context-dependent attackers to cause a denial of service (memory consumption) via a large number of crafted XML files that cause improperly-handled reallocation failures when expanding entities.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libexpat1 2.0.1-0ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2013-10-22-3
BID	52379
CVE	CVE-2012-0876
CVE	CVE-2012-1148
DEBIAN	DSA-2525
DISA_SEVERITY	Category I
DISA_VMSKEY	V0035032
IAVM	2012-A-0189
REDHAT	RHSA-2012:0731
USN	USN-1527-1

Vulnerability Solution:

- lib64expat1 on Ubuntu Linux 10.04

Upgrade lib64expat1 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade lib64expat1 to the latest version

•lib64expat1 on Ubuntu Linux 11.04

Upgrade lib64expat1 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade lib64expat1 to the latest version

•lib64expat1 on Ubuntu Linux 11.10

Upgrade lib64expat1 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade lib64expat1 to the latest version

•lib64expat1 on Ubuntu Linux 12.04

Upgrade lib64expat1 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade lib64expat1 to the latest version

•lib64expat1 on Ubuntu Linux 8.04

Upgrade lib64expat1 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade lib64expat1 to the latest version

•libexpat1 on Ubuntu Linux 10.04

Upgrade libexpat1 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libexpat1 to the latest version

•libexpat1 on Ubuntu Linux 11.04

Upgrade libexpat1 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libexpat1 to the latest version

•libexpat1 on Ubuntu Linux 11.10

Upgrade libexpat1 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libexpat1 to the latest version

•libexpat1 on Ubuntu Linux 12.04

Upgrade libexpat1 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libexpat1 to the latest version

•libexpat1 on Ubuntu Linux 8.04

Upgrade libexpat1 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libexpat1 to the latest version

•libexpat1-udeb on Ubuntu Linux 10.04

Upgrade libexpat1-udeb for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libexpat1-udeb to the latest version

•libexpat1-udeb on Ubuntu Linux 11.04

Upgrade libexpat1-udeb for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libexpat1-udeb to the latest version

•libexpat1-udeb on Ubuntu Linux 11.10

Upgrade libexpat1-udeb for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libexpat1-udeb to the latest version

•libexpat1-udeb on Ubuntu Linux 12.04

Upgrade libexpat1-udeb for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libexpat1-udeb to the latest version

•libexpat1-udeb on Ubuntu Linux 8.04

Upgrade libexpat1-udeb for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libexpat1-udeb to the latest version

3.2.151. USN-1542-1: PostgreSQL vulnerabilities (ubuntu-usn-1542-1)

Description:

The libxslt support in contrib/xml2 in PostgreSQL 8.3 before 8.3.20, 8.4 before 8.4.13, 9.0 before 9.0.9, and 9.1 before 9.1.5 does not properly restrict access to files and URLs, which allows remote authenticated users to modify data, obtain sensitive information, or trigger outbound traffic to arbitrary external hosts by leveraging (1) stylesheet commands that are permitted by the libxslt security options or (2) an xslt_process feature, related to an XML External Entity (aka XXE) issue.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu postgresql-8.3 8.3.1-1

References:

Source	Reference
APPLE	APPLE-SA-2013-03-14-1
BID	55072
BID	55074
CVE	CVE-2012-3488
CVE	CVE-2012-3489
DEBIAN	DSA-2534
REDHAT	RHSA-2012:1263
REDHAT	RHSA-2012:1264
USN	USN-1542-1

Vulnerability Solution:

- postgresql-8.3 on Ubuntu Linux 8.04
Upgrade postgresql-8.3 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version
- postgresql-8.4 on Ubuntu Linux 10.04
Upgrade postgresql-8.4 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version
- postgresql-8.4 on Ubuntu Linux 11.04
Upgrade postgresql-8.4 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version

- postgresql-9.1 on Ubuntu Linux 11.10
Upgrade postgresql-9.1 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade postgresql-9.1 to the latest version
- postgresql-9.1 on Ubuntu Linux 12.04
Upgrade postgresql-9.1 for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade postgresql-9.1 to the latest version

3.2.152. USN-1546-1: libgc vulnerability (ubuntu-usn-1546-1)

Description:

Multiple integer overflows in the (1) GC_generic_malloc and (2) calloc funtions in malloc.c, and the (3) GC_generic_malloc_ignore_off_page function in mallocx.c in Boehm-Demers-Weiser GC (libgc) before 7.2 make it easier for context-dependent attackers to perform memory-related attacks such as buffer overflows via a large size value, which causes less memory to be allocated than expected.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libgc1c2 1:6.8-1.1

References:

Source	Reference
BID	54227
CVE	CVE-2012-2673
REDHAT	RHSA-2013:1500
REDHAT	RHSA-2014:0149
REDHAT	RHSA-2014:0150
USN	USN-1546-1

Vulnerability Solution:

- libgc1c2 on Ubuntu Linux 10.04
Upgrade libgc1c2 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libgc1c2 to the latest version
- libgc1c2 on Ubuntu Linux 11.04
Upgrade libgc1c2 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade libgc1c2 to the latest version
- libgc1c2 on Ubuntu Linux 11.10
Upgrade libgc1c2 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libgc1c2 to the latest version

- libgc1c2 on Ubuntu Linux 12.04

Upgrade libgc1c2 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libgc1c2 to the latest version

- libgc1c2 on Ubuntu Linux 8.04

Upgrade libgc1c2 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libgc1c2 to the latest version

3.2.153. USN-1732-1: OpenSSL vulnerabilities (ubuntu-usn-1732-1)

Description:

OpenSSL before 0.9.8y, 1.0.0 before 1.0.0k, and 1.0.1 before 1.0.1d does not properly perform signature verification for OCSP responses, which allows remote OCSP servers to cause a denial of service (NULL pointer dereference and application crash) via an invalid key.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libssl0.9.8 0.9.8g-4ubuntu3.18

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
BID	57755
CERT	TA13-051A
CERT-VN	737740
CVE	CVE-2012-2686
CVE	CVE-2013-0166
CVE	CVE-2013-0169
DEBIAN	DSA-2621
DEBIAN	DSA-2622
OVAL	OVAL18754
OVAL	OVAL18841
OVAL	OVAL18868
OVAL	OVAL19016

Source	Reference
OVAL	OVAL19081
OVAL	OVAL19360
OVAL	OVAL19424
OVAL	OVAL19487
OVAL	OVAL19540
OVAL	OVAL19608
OVAL	OVAL19660
REDHAT	RHSA-2013:0587
REDHAT	RHSA-2013:0782
REDHAT	RHSA-2013:0783
REDHAT	RHSA-2013:0833
REDHAT	RHSA-2013:1455
REDHAT	RHSA-2013:1456
USN	USN-1732-1

Vulnerability Solution:

- libssl0.9.8 on Ubuntu Linux 10.04

Upgrade libssl0.9.8 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libssl0.9.8 to the latest version

- libssl0.9.8 on Ubuntu Linux 8.04

Upgrade libssl0.9.8 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libssl0.9.8 to the latest version

- libssl1.0.0 on Ubuntu Linux 11.10

Upgrade libssl1.0.0 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libssl1.0.0 to the latest version

- libssl1.0.0 on Ubuntu Linux 12.04

Upgrade libssl1.0.0 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libssl1.0.0 to the latest version

- libssl1.0.0 on Ubuntu Linux 12.10

Upgrade libssl1.0.0 for Ubuntu 12.10

Use `apt-get upgrade` to upgrade libssl1.0.0 to the latest version

3.2.154. USN-1765-1: Apache HTTP Server vulnerabilities (ubuntu-usn-1765-1)

Description:

The mod_proxy_ajp module in the Apache HTTP Server 2.2.12 through 2.2.21 places a worker node into an error state upon detection of a long request-processing time, which allows remote attackers to cause a denial of service (worker consumption) via an expensive request.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu apache2.2-common 2.2.8-1ubuntu0.15

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
BID	64758
CVE	CVE-2012-3499
CVE	CVE-2012-4557
CVE	CVE-2012-4558
CVE	CVE-2013-1048
DEBIAN	DSA-2579
DEBIAN	DSA-2637
DISA_SEVERITY	Category I
DISA_VMSKEY	V0040288
IAVM	2013-A-0177
OVAL	OVAL18938
OVAL	OVAL18977
OVAL	OVAL19284
OVAL	OVAL19312
REDHAT	RHSA-2013:0815
REDHAT	RHSA-2013:1207
REDHAT	RHSA-2013:1208
REDHAT	RHSA-2013:1209
USN	USN-1765-1

Vulnerability Solution:

- apache2.2-common on Ubuntu Linux 10.04
Upgrade apache2.2-common for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade apache2.2-common to the latest version
- apache2.2-common on Ubuntu Linux 11.10
Upgrade apache2.2-common for Ubuntu 11.10

Use `apt-get upgrade` to upgrade apache2.2-common to the latest version

- apache2.2-common on Ubuntu Linux 12.04

Upgrade apache2.2-common for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade apache2.2-common to the latest version

- apache2.2-common on Ubuntu Linux 12.10

Upgrade apache2.2-common for Ubuntu 12.10

Use `apt-get upgrade` to upgrade apache2.2-common to the latest version

- apache2.2-common on Ubuntu Linux 8.04

Upgrade apache2.2-common for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade apache2.2-common to the latest version

3.2.155. USN-1801-1: curl vulnerability (ubuntu-usn-1801-1)

Description:

The tailMatch function in cookie.c in cURL and libcurl before 7.30.0 does not properly match the path domain when sending cookies, which allows remote attackers to steal cookies via a matching suffix in the domain of a URL.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libcurl3 7.18.0-1ubuntu2.3

References:

Source	Reference
APPLE	APPLE-SA-2013-10-22-3
BID	59058
CVE	CVE-2013-1944
DEBIAN	DSA-2660
OSVDB	92316
REDHAT	RHSA-2013:0771
USN	USN-1801-1

Vulnerability Solution:

- curl on Ubuntu Linux 10.04

Upgrade curl for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade curl to the latest version

- curl on Ubuntu Linux 11.10

Upgrade curl for Ubuntu 11.10

Use `apt-get upgrade` to upgrade curl to the latest version

- curl on Ubuntu Linux 12.04
Upgrade curl for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade curl to the latest version
- curl on Ubuntu Linux 12.10
Upgrade curl for Ubuntu 12.10
Use `apt-get upgrade` to upgrade curl to the latest version
- curl on Ubuntu Linux 8.04
Upgrade curl for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade curl to the latest version
- libcurl3 on Ubuntu Linux 10.04
Upgrade libcurl3 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libcurl3 to the latest version
- libcurl3 on Ubuntu Linux 11.10
Upgrade libcurl3 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade libcurl3 to the latest version
- libcurl3 on Ubuntu Linux 12.04
Upgrade libcurl3 for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade libcurl3 to the latest version
- libcurl3 on Ubuntu Linux 12.10
Upgrade libcurl3 for Ubuntu 12.10
Use `apt-get upgrade` to upgrade libcurl3 to the latest version
- libcurl3 on Ubuntu Linux 8.04
Upgrade libcurl3 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libcurl3 to the latest version

3.2.156. USN-653-1: D-Bus vulnerabilities (ubuntu-usn-653-1)

Description:

dbus-daemon in D-Bus before 1.0.3, and 1.1.x before 1.1.20, recognizes send_interface attributes in allow directives in the security policy only for fully qualified method calls, which allows local users to bypass intended access restrictions via a method call with a NULL interface.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libdbus-1-3 1.1.20-1ubuntu1

References:

Source	Reference
BID	28023
BID	31602
CVE	CVE-2008-0595
CVE	CVE-2008-3834
DEBIAN	DSA-1599
DEBIAN	DSA-1658
OVAL	OVAL10253
OVAL	OVAL9353
REDHAT	RHSA-2008:0159
REDHAT	RHSA-2009:0008
USN	USN-653-1
XF	45701

Vulnerability Solution:

•libdbus-1-3 on Ubuntu Linux 7.04

Upgrade libdbus-1-3 for Ubuntu 7.04

Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version

•libdbus-1-3 on Ubuntu Linux 7.10

Upgrade libdbus-1-3 for Ubuntu 7.10

Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version

•libdbus-1-3 on Ubuntu Linux 8.04

Upgrade libdbus-1-3 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version

3.2.157. USN-671-1: MySQL vulnerabilities (ubuntu-usn-671-1)*Description:*

MySQL before 5.0.67 allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are originally associated with pathnames without symlinks, and that can point to tables created at a future time at which a pathname is modified to contain a symlink to a subdirectory of the MySQL home data directory. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-4097.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04

Affected Nodes:	Additional Information:
	Vulnerable software installed: Ubuntu mysql-server-5.0 5.0.51a-3ubuntu5

References:

Source	Reference
APPLE	APPLE-SA-2008-10-09
APPLE	APPLE-SA-2009-09-10-2
BID	29106
BID	31681
CVE	CVE-2008-2079
CVE	CVE-2008-3963
CVE	CVE-2008-4097
CVE	CVE-2008-4098
DEBIAN	DSA-1608
DEBIAN	DSA-1662
DEBIAN	DSA-1783
OVAL	OVAL10133
OVAL	OVAL10521
OVAL	OVAL10591
REDHAT	RHSA-2008:0505
REDHAT	RHSA-2008:0510
REDHAT	RHSA-2008:0768
REDHAT	RHSA-2009:1067
REDHAT	RHSA-2009:1289
REDHAT	RHSA-2010:0110
USN	USN-671-1
XF	42267
XF	45042
XF	45648
XF	45649

Vulnerability Solution:

- mysql-server-5.0 on Ubuntu Linux 7.10

Upgrade mysql-server-5.0 for Ubuntu 7.10

Use `apt-get upgrade` to upgrade mysql-server-5.0 to the latest version

- mysql-server-5.0 on Ubuntu Linux 8.04

Upgrade mysql-server-5.0 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade mysql-server-5.0 to the latest version

3.2.158. USN-837-1: Newt vulnerability (ubuntu-usn-837-1)

Description:

Heap-based buffer overflow in textbox.c in newt 0.51.5, 0.51.6, and 0.52.2 allows local users to cause a denial of service (application crash) or possibly execute arbitrary code via a request to display a crafted text dialog box.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libnewt0.52 0.52.2-11.2ubuntu1

References:

Source	Reference
BID	36515
CVE	CVE-2009-2905
DEBIAN	DSA-1894
OVAL	OVAL8556
OVAL	OVAL9664
REDHAT	RHSA-2009:1463
USN	USN-837-1

Vulnerability Solution:

- libnewt0.52 on Ubuntu Linux 8.04

Upgrade libnewt0.52 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libnewt0.52 to the latest version

- libnewt0.52 on Ubuntu Linux 8.10

Upgrade libnewt0.52 for Ubuntu 8.10

Use `apt-get upgrade` to upgrade libnewt0.52 to the latest version

- libnewt0.52 on Ubuntu Linux 9.04

Upgrade libnewt0.52 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade libnewt0.52 to the latest version

3.2.159. USN-890-1: Expat vulnerabilities (ubuntu-usn-890-1)

Description:

The updatePosition function in lib/xmltok_impl.c in libexpat in Expat 2.0.1, as used in Python, PyXML, w3c-libwww, and other software, allows context-dependent attackers to cause a denial of service (application crash) via an XML document with crafted UTF-8 sequences that trigger a buffer over-read, a different vulnerability than CVE-2009-2625.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libexpat1 2.0.1-0ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2009-09-03-1
BID	35958
BID	37203
CERT	TA09-294A
CERT	TA10-012A
CVE	CVE-2009-2625
CVE	CVE-2009-3560
CVE	CVE-2009-3720
DEBIAN	DSA-1953
DEBIAN	DSA-1984
DISA_SEVERITY	Category I
DISA_VMSKEY	V0031252
IAVM	2012-A-0020
OVAL	OVAL10613
OVAL	OVAL11019
OVAL	OVAL12719
OVAL	OVAL12942
OVAL	OVAL6883
OVAL	OVAL7112
OVAL	OVAL8520
OVAL	OVAL9356

Source	Reference
REDHAT	RHSA-2009:1199
REDHAT	RHSA-2009:1200
REDHAT	RHSA-2009:1201
REDHAT	RHSA-2009:1615
REDHAT	RHSA-2009:1636
REDHAT	RHSA-2009:1637
REDHAT	RHSA-2009:1649
REDHAT	RHSA-2009:1650
REDHAT	RHSA-2010:0002
REDHAT	RHSA-2011:0858
REDHAT	RHSA-2011:0896
REDHAT	RHSA-2012:1232
REDHAT	RHSA-2012:1537
SUSE	SUSE-SA:2009:053
USN	USN-890-1

Vulnerability Solution:

- lib64expat1 on Ubuntu Linux 8.04

Upgrade lib64expat1 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade lib64expat1 to the latest version

- lib64expat1 on Ubuntu Linux 8.10

Upgrade lib64expat1 for Ubuntu 8.10

Use `apt-get upgrade` to upgrade lib64expat1 to the latest version

- lib64expat1 on Ubuntu Linux 9.04

Upgrade lib64expat1 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade lib64expat1 to the latest version

- lib64expat1 on Ubuntu Linux 9.10

Upgrade lib64expat1 for Ubuntu 9.10

Use `apt-get upgrade` to upgrade lib64expat1 to the latest version

- libexpat1 on Ubuntu Linux 8.04

Upgrade libexpat1 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libexpat1 to the latest version

- libexpat1 on Ubuntu Linux 8.10

Upgrade libexpat1 for Ubuntu 8.10

Use `apt-get upgrade` to upgrade libexpat1 to the latest version

- libexpat1 on Ubuntu Linux 9.04

Upgrade libexpat1 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade libexpat1 to the latest version

- libexpat1 on Ubuntu Linux 9.10

Upgrade libexpat1 for Ubuntu 9.10

Use `apt-get upgrade` to upgrade libexpat1 to the latest version

- libexpat1-udeb on Ubuntu Linux 8.04

Upgrade libexpat1-udeb for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libexpat1-udeb to the latest version

- libexpat1-udeb on Ubuntu Linux 8.10

Upgrade libexpat1-udeb for Ubuntu 8.10

Use `apt-get upgrade` to upgrade libexpat1-udeb to the latest version

- libexpat1-udeb on Ubuntu Linux 9.04

Upgrade libexpat1-udeb for Ubuntu 9.04

Use `apt-get upgrade` to upgrade libexpat1-udeb to the latest version

- libexpat1-udeb on Ubuntu Linux 9.10

Upgrade libexpat1-udeb for Ubuntu 9.10

Use `apt-get upgrade` to upgrade libexpat1-udeb to the latest version

3.2.160. USN-986-1: bzip2 vulnerability (ubuntu-usn-986-1)

Description:

Integer overflow in the BZ2_decompress function in decompress.c in bzip2 and libbzip2 before 1.0.6 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted compressed file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libbz2-1.0 1.0.4-2ubuntu4

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
CVE	CVE-2010-0405
DISA_SEVERITY	Category II
DISA_VMSKEY	V0025411
IAVM	2010-B-0083
REDHAT	RHSA-2010:0703
REDHAT	RHSA-2010:0858

Source	Reference
USN	USN-986-1

Vulnerability Solution:

•bzip2 on Ubuntu Linux 10.04

Upgrade bzip2 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade bzip2 to the latest version

•bzip2 on Ubuntu Linux 8.04

Upgrade bzip2 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade bzip2 to the latest version

•bzip2 on Ubuntu Linux 9.04

Upgrade bzip2 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade bzip2 to the latest version

•bzip2 on Ubuntu Linux 9.10

Upgrade bzip2 for Ubuntu 9.10

Use `apt-get upgrade` to upgrade bzip2 to the latest version

•libbz2-1.0 on Ubuntu Linux 10.04

Upgrade libbz2-1.0 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libbz2-1.0 to the latest version

•libbz2-1.0 on Ubuntu Linux 8.04

Upgrade libbz2-1.0 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libbz2-1.0 to the latest version

•libbz2-1.0 on Ubuntu Linux 9.04

Upgrade libbz2-1.0 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade libbz2-1.0 to the latest version

•libbz2-1.0 on Ubuntu Linux 9.10

Upgrade libbz2-1.0 for Ubuntu 9.10

Use `apt-get upgrade` to upgrade libbz2-1.0 to the latest version

3.2.161. USN-986-3: dpkg vulnerability (ubuntu-usn-986-3)*Description:*

Integer overflow in the BZ2_decompress function in decompress.c in bzip2 and libbzip2 before 1.0.6 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted compressed file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu dpkg 1.14.16.6ubuntu3

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
CVE	CVE-2010-0405
DISA_SEVERITY	Category II
DISA_VMSKEY	V0025411
IAVM	2010-B-0083
REDHAT	RHSA-2010:0703
REDHAT	RHSA-2010:0858
USN	USN-986-3

Vulnerability Solution:

- dpkg on Ubuntu Linux 10.04
Upgrade dpkg for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade dpkg to the latest version
- dpkg on Ubuntu Linux 8.04
Upgrade dpkg for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade dpkg to the latest version
- dpkg on Ubuntu Linux 9.04
Upgrade dpkg for Ubuntu 9.04
Use `apt-get upgrade` to upgrade dpkg to the latest version
- dpkg on Ubuntu Linux 9.10
Upgrade dpkg for Ubuntu 9.10
Use `apt-get upgrade` to upgrade dpkg to the latest version

3.2.162. Apache HTTPD: error responses can expose cookies (CVE-2012-0053) (apache-httpd-cve-2012-0053)*Description:*

A flaw was found in the default error response for status code 400. This flaw could be used by an attacker to expose "httpOnly" cookies when no custom ErrorDocument is specified.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceHTTP GET request to http://192.168.0.102/ HTTP response code was an expected 400 9: <h1>Bad Request</h1> 10: <p>Your browser sent a request that this server could not understand... 11: Request header field is missing ':' separator.

Affected Nodes:	Additional Information:
	12: <pre> 9: R7TESTR7TESTR7TESTR7TESTR7TESTR7TESTR7TESTR7TESTR7TESTR7TESTR7TE...

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
BID	51706
CVE	CVE-2012-0053
REDHAT	RHSA-2012:0128
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.65

Upgrade to Apache HTTPD version 2.0.65

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.2 and < 2.2.22

Upgrade to Apache HTTPD version 2.2.22

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.163. Apache HTTPD: mod_deflate denial of service (CVE-2014-0118) (apache-httpd-cve-2014-0118)*Description:*

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_deflate. Review your web server configuration for validation. A resource consumption flaw was found in mod_deflate. If request body decompression was configured (using the "DEFLATE" input filter), a remote attacker could cause the server to consume significant memory and/or CPU resources. The use of request body decompression is not a common configuration.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
BID	68745
CVE	CVE-2014-0118
DEBIAN	DSA-2989
DISA_SEVERITY	Category I
DISA_VMSKEY	V0053307
IAVM	2014-A-0114
REDHAT	RHSA-2014:1019
REDHAT	RHSA-2014:1020
REDHAT	RHSA-2014:1021
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.29

Upgrade to Apache HTTPD version 2.2.29

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.29.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.10

Upgrade to Apache HTTPD version 2.4.10

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.10.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.164. ISC BIND: DNSSEC validation code could cause bogus NXDOMAIN responses (CVE-2010-0097) (dns-bind-cve-2010-0097)

Description:

ISC BIND 9.0.x through 9.3.x, 9.4 before 9.4.3-P5, 9.5 before 9.5.2-P2, 9.6 before 9.6.1-P3, and 9.7.0 beta does not properly validate DNSSEC (1) NSEC and (2) NSEC3 records, which allows remote attackers to add the Authenticated Data (AD) flag to a forged NXDOMAIN response for an existing domain.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	37865
CERT-VN	360341
CVE	CVE-2010-0097
DEBIAN	DSA-2054
OSVDB	61853
OVAL	OVAL12205
OVAL	OVAL7212
OVAL	OVAL7430
OVAL	OVAL9357
REDHAT	RHSA-2010:0062
REDHAT	RHSA-2010:0095
SUSE	SUSE-SA:2010:008
URL	https://kb.isc.org/article/AA-00932/0
URL	https://kb.isc.org/article/AA-00932/187/CVE-2010-0097%3A-BIND-9-DNSSEC-validation-code-could-cause-bogus-NXDOMAIN-responses.html
XF	55753

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the [ISC website](#).

3.2.165. ISC BIND: cache incorrectly allows an ncache entry and an RRSIG for the same type (CVE-2010-3613) (dns-bind-cve-2010-3613)

Description:

named in ISC BIND 9.6.2 before 9.6.2-P3, 9.6-ESV before 9.6-ESV-R3, and 9.7.x before 9.7.2-P3 does not properly handle the combination of signed negative responses and corresponding RRSIG records in the cache, which allows remote attackers to cause a denial of service (daemon crash) via a query for cached data.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	45133
CERT-VN	706148
CVE	CVE-2010-3613
DEBIAN	DSA-2130
DISA_SEVERITY	Category I
DISA_VMSKEY	V0027158
IAVM	2011-A-0066
NETBSD	NetBSD-SA2011-001
OSVDB	69558
OVAL	OVAL12601
REDHAT	RHSA-2010:0975
REDHAT	RHSA-2010:0976
REDHAT	RHSA-2010:1000
URL	https://kb.isc.org/article/AA-00938/0
URL	https://kb.isc.org/article/AA-00938/187/CVE-2010-3613%3A-cache-incorrectly-allows-a-ncache-entry-and-a-rrsig-for-the-same-type.html

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the [ISC website](#).

3.2.166. MySQL Bug #29908: ALTER VIEW Privilege Escalation Vulnerability (mysql-bug-29908-alter-view-priv-esc)

Description:

A flaw in the ALTER VIEW routine of MySQL allows for the opportunity of an authenticated user to elevate their privileges in certain contexts.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
URL	http://bugs.mysql.com/bug.php?id=29908

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.52

Upgrade to Oracle MySQL version 5.0.52

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.23

Upgrade to Oracle MySQL version 5.1.23

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.167. MySQL Bug #44798: Stored Procedures Server Crash (mysql-bug-44798-stored-procedures-server-crash)*Description:*

Versions of MySQL server 5.0 before 5.0.84 and 5.1 before 5.1.36 suffer from a privilege interpretation flaw that causes a server crash. A user created with the privileges to create stored procedures but not execute them will trigger this issue.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
URL	http://bugs.mysql.com/bug.php?id=44798

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.84

Upgrade to Oracle MySQL version 5.0.84

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.36

Upgrade to Oracle MySQL version 5.1.36

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.168. Oracle MySQL Vulnerability: CVE-2010-3677 (oracle-mysql-cve-2010-3677)*Description:*

Oracle MySQL 5.1 before 5.1.49 and 5.0 before 5.0.92 allows remote authenticated users to cause a denial of service (mysqld daemon crash) via a join query that uses a table with a unique SET column.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
APPLE	APPLE-SA-2011-06-23-1
BID	42646
CVE	CVE-2010-3677
DEBIAN	DSA-2143
REDHAT	RHSA-2010:0825
REDHAT	RHSA-2011:0164
XF	64688

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.92

Upgrade to Oracle MySQL version 5.0.92

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.49

Upgrade to Oracle MySQL version 5.1.49

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.169. Oracle MySQL Vulnerability: CVE-2010-3682 (oracle-mysql-cve-2010-3682)*Description:*

Oracle MySQL 5.1 before 5.1.49 and 5.0 before 5.0.92 allows remote authenticated users to cause a denial of service (mysqld daemon crash) by using EXPLAIN with crafted "SELECT ... UNION ... ORDER BY (SELECT ... WHERE ...)" statements, which triggers a NULL pointer dereference in the Item_singlerow_subselect::store function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
APPLE	APPLE-SA-2011-06-23-1
BID	42599
CVE	CVE-2010-3682
DEBIAN	DSA-2143
REDHAT	RHSA-2010:0825
REDHAT	RHSA-2011:0164
XF	64684

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.92

Upgrade to Oracle MySQL version 5.0.92

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.49

Upgrade to Oracle MySQL version 5.1.49

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.170. Oracle MySQL Vulnerability: CVE-2010-3834 (oracle-mysql-cve-2010-3834)

Description:

Unspecified vulnerability in MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (server crash) via vectors related to "materializing a derived table that required a temporary table for grouping" and "user variable assignments."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
APPLE	APPLE-SA-2011-06-23-1
BID	43676
CVE	CVE-2010-3834
DEBIAN	DSA-2143
XF	64844

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.92

Upgrade to Oracle MySQL version 5.0.92

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.51

Upgrade to Oracle MySQL version 5.1.51

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for

example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.5 and < 5.5.6

Upgrade to Oracle MySQL version 5.5.6

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.171. Oracle MySQL Vulnerability: CVE-2010-3836 (oracle-mysql-cve-2010-3836)

Description:

MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (assertion failure and server crash) via vectors related to view preparation, pre-evaluation of LIKE predicates, and IN Optimizers.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
APPLE	APPLE-SA-2011-06-23-1
BID	43676
CVE	CVE-2010-3836
DEBIAN	DSA-2143
REDHAT	RHSA-2010:0825
REDHAT	RHSA-2011:0164
XF	64842

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.92

Upgrade to Oracle MySQL version 5.0.92

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.51

Upgrade to Oracle MySQL version 5.1.51

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.6

Upgrade to Oracle MySQL version 5.5.6

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.172. Oracle MySQL Vulnerability: CVE-2010-3837 (oracle-mysql-cve-2010-3837)

Description:

MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (server crash) via a prepared statement that uses GROUP_CONCAT with the WITH ROLLUP modifier, probably triggering a use-after-free error when a copied object is modified in a way that also affects the original object.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
APPLE	APPLE-SA-2011-06-23-1
BID	43676
CVE	CVE-2010-3837
DEBIAN	DSA-2143
REDHAT	RHSA-2010:0825
REDHAT	RHSA-2011:0164
XF	64841

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.92

Upgrade to Oracle MySQL version 5.0.92

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.51

Upgrade to Oracle MySQL version 5.1.51

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.5 and < 5.5.6

Upgrade to Oracle MySQL version 5.5.6

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.173. Oracle MySQL Vulnerability: CVE-2010-3838 (oracle-mysql-cve-2010-3838)

Description:

MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (server crash) via a query that uses the (1) GREATEST or (2) LEAST function with a mixed list of numeric and LONGBLOB arguments, which is not properly handled when the function's result is "processed using an intermediate temporary table."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
APPLE	APPLE-SA-2011-06-23-1
BID	43676
CVE	CVE-2010-3838
DEBIAN	DSA-2143
REDHAT	RHSA-2010:0825
REDHAT	RHSA-2011:0164
XF	64840

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.92

Upgrade to Oracle MySQL version 5.0.92

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for

example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.51

Upgrade to Oracle MySQL version 5.1.51

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.5 and < 5.5.6

Upgrade to Oracle MySQL version 5.5.6

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.174. Oracle MySQL Vulnerability: CVE-2012-0087 (oracle-mysql-cve-2012-0087)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x and 5.1.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0101 and CVE-2012-0102.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
BID	51509
CVE	CVE-2012-0087
OSVDB	78377
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72519

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.175. Oracle MySQL Vulnerability: CVE-2012-0101 (oracle-mysql-cve-2012-0101)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x and 5.1.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0087 and CVE-2012-0102.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0101
OSVDB	78378
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72520

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.176. Oracle MySQL Vulnerability: CVE-2012-0102 (oracle-mysql-cve-2012-0102)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x and 5.1.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0087 and CVE-2012-0101.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0102
OSVDB	78379
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72521

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.177. Oracle MySQL Vulnerability: CVE-2012-0112 (oracle-mysql-cve-2012-0112)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, CVE-2012-0485, and CVE-2012-0492.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0112
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.178. Oracle MySQL Vulnerability: CVE-2012-0115 (oracle-mysql-cve-2012-0115)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0119, CVE-2012-0120, CVE-2012-0485, and CVE-2012-0492.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0115
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.179. Oracle MySQL Vulnerability: CVE-2012-0117 (oracle-mysql-cve-2012-0117)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0491, CVE-2012-0493, and CVE-2012-0495.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0117
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.180. Oracle MySQL Vulnerability: CVE-2012-0119 (oracle-mysql-cve-2012-0119)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0120, CVE-2012-0485, and CVE-2012-0492.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0119
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.181. Oracle MySQL Vulnerability: CVE-2012-0120 (oracle-mysql-cve-2012-0120)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0119, CVE-2012-0485, and CVE-2012-0492.

Affected Nodes:

Affected Nodes:	Additional Information:
-----------------	-------------------------

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0120
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.182. Oracle MySQL Vulnerability: CVE-2012-0484 (oracle-mysql-cve-2012-0484)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows remote authenticated users to affect confidentiality via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
BID	51515
CVE	CVE-2012-0484
OSVDB	78372
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72525

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.183. Oracle MySQL Vulnerability: CVE-2012-0485 (oracle-mysql-cve-2012-0485)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, and CVE-2012-0492.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
BID	51513
CVE	CVE-2012-0485
OSVDB	78383
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72526

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.184. Oracle MySQL Vulnerability: CVE-2012-0487 (oracle-mysql-cve-2012-0487)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0488, CVE-2012-0489, CVE-2012-0491, CVE-2012-0493, and CVE-2012-0495.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
BID	51503
CVE	CVE-2012-0487
OSVDB	78385
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72528

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.185. Oracle MySQL Vulnerability: CVE-2012-0488 (oracle-mysql-cve-2012-0488)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0487, CVE-2012-0489, CVE-2012-0491, CVE-2012-0493, and CVE-2012-0495.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
BID	51506
CVE	CVE-2012-0488
OSVDB	78386
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72529

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.186. Oracle MySQL Vulnerability: CVE-2012-0489 (oracle-mysql-cve-2012-0489)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0491, CVE-2012-0493, and CVE-2012-0495.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
BID	51510
CVE	CVE-2012-0489
OSVDB	78387
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72530

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.187. Oracle MySQL Vulnerability: CVE-2012-0490 (oracle-mysql-cve-2012-0490)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows remote authenticated users to affect availability via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
BID	51524
CVE	CVE-2012-0490
OSVDB	78388
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72531

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.188. Oracle MySQL Vulnerability: CVE-2012-0491 (oracle-mysql-cve-2012-0491)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0493, and CVE-2012-0495.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
BID	51518
CVE	CVE-2012-0491
OSVDB	78389
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72532

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.189. Oracle MySQL Vulnerability: CVE-2012-0495 (oracle-mysql-cve-2012-0495)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0491, and CVE-2012-0493.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0495
OSVDB	78390
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72533

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.190. PHP Vulnerability: CVE-2007-4887 (php-cve-2007-4887)*Description:*

The dl function in PHP 5.2.4 and earlier allows context-dependent attackers to cause a denial of service (application crash) via a long string in the library parameter. NOTE: there are limited usage scenarios under which this would be a vulnerability.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference

Source	Reference
APPLE	APPLE-SA-2008-03-18
BID	26403
CVE	CVE-2007-4887
OVAL	OVAL5767

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.5.tar.gz>

3.2.191. PHP Vulnerability: CVE-2007-5447 (php-cve-2007-5447)*Description:*

ioncube_loader_win_5.2.dll in the ionCube Loader 6.5 extension for PHP 5.2.4 does not follow `safe_mode` and `disable_functions` restrictions, which allows context-dependent attackers to bypass intended limitations, as demonstrated by reading arbitrary files via the `ioncube_read_file` function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
BID	26024
CVE	CVE-2007-5447
OSVDB	41708
XF	37227

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.5.tar.gz>

3.2.192. PHP Vulnerability: CVE-2011-0753 (php-cve-2011-0753)*Description:*

Race condition in the PCNTL extension in PHP before 5.3.4, when a user-defined signal handler exists, might allow context-dependent attackers to cause a denial of service (memory corruption) via a large number of concurrent signals.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2011-0753
OVAL	OVAL12271
XF	65431

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.3.4.tar.gz>

3.2.193. PHP Vulnerability: CVE-2011-1398 (php-cve-2011-1398)*Description:*

The sapi_header_op function in main/SAPI.c in PHP before 5.3.11 and 5.4.x before 5.4.0RC2 does not check for %0D sequences (aka carriage return characters), which allows remote attackers to bypass an HTTP response-splitting protection mechanism via a crafted URL, related to improper interaction between the PHP header function and certain browsers, as demonstrated by Internet Explorer and Google Chrome.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2011-1398
REDHAT	RHSA-2013:1307

Vulnerability Solution:

- Upgrade to PHP version 5.3.11

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 5.4.0

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.194. PHP Fixed possible attack in SSL sockets with SSL 3.0 / TLS 1.0 (php-cve-2011-3389)

Description:

The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-1
APPLE	APPLE-SA-2011-10-12-2
APPLE	APPLE-SA-2012-02-01-1
APPLE	APPLE-SA-2012-05-09-1
APPLE	APPLE-SA-2012-07-25-2
APPLE	APPLE-SA-2012-09-19-2
APPLE	APPLE-SA-2013-10-22-3
BID	49388
BID	49778
CERT	TA12-010A
CERT-VN	864643
CVE	CVE-2011-3389
DISA_SEVERITY	Category I
DISA_VMSKEY	V0031054
IAVM	2012-B-0006
MS	MS12-006
OSVDB	74829
OVAL	OVAL14752
REDHAT	RHSA-2011:1384
REDHAT	RHSA-2012:0006
REDHAT	RHSA-2013:1455

Vulnerability Solution:

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.195. PHP Vulnerability: CVE-2012-2143 (php-cve-2012-2143)*Description:*

The crypt_des (aka DES-based crypt) function in FreeBSD before 9.0-RELEASE-p2, as used in PHP, PostgreSQL, and other products, does not process the complete cleartext password if this password contains a 0x80 character, which makes it easier for context-dependent attackers to obtain access via an authentication attempt with an initial substring of the intended password, as demonstrated by a Unicode password.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
CVE	CVE-2012-2143
DEBIAN	DSA-2491
REDHAT	RHSA-2012:1037

Vulnerability Solution:

- Upgrade to PHP version 5.3.14

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 5.4.4

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.196. PHP Vulnerability: CVE-2014-2497 (php-cve-2014-2497)*Description:*

The gdImageCreateFromXpm function in gdxpm.c in libgd, as used in PHP 5.4.26 and earlier, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted color table in an XPM file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8

Affected Nodes:	Additional Information:
	Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
CVE	CVE-2014-2497
DEBIAN	DSA-3215
REDHAT	RHSA-2014:1326
REDHAT	RHSA-2014:1327
REDHAT	RHSA-2014:1765
REDHAT	RHSA-2014:1766

Vulnerability Solution:

- Upgrade to PHP version 5.3.28

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 5.5.0

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.197. PHP Vulnerability: CVE-2014-5459 (php-cve-2014-5459)*Description:*

The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2014-5459

Vulnerability Solution:

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.198. PHP Fixed dl() to limit argument size to MAXPATHLEN (php-fixed-dl-to-limit-argument-size-to-maxpathlen)

Description:

The dl function in PHP 5.2.4 and earlier allows context-dependent attackers to cause a denial of service (application crash) via a long string in the library parameter. NOTE: there are limited usage scenarios under which this would be a vulnerability.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP service Product HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2008-03-18
BID	26403
CVE	CVE-2007-4887
OVAL	OVAL5767

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.5.tar.gz>

3.2.199. Unencrypted Telnet Service Available (telnet-open-port)*Description:*

Telnet is an unencrypted protocol, as such it sends sensitive data (usernames, passwords) in clear text.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:23	Running Telnet service

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

Vulnerability Solution:

Disable the telnet service. Replace it with technologies such as SSH, VPN, or TLS.

3.2.200. USN-1009-2: GNU C Library vulnerability (ubuntu-usn-1009-2)

Description:

USN-1009-1 fixed vulnerabilities in the GNU C library. Colin Watson discovered that the fixes were incomplete and introduced flaws with `setuid` programs loading libraries that used dynamic string tokens in their `RPATH`. If the "man" program was installed `setuid`, a local attacker could exploit this to gain "man" user privileges, potentially leading to further privilege escalations. Default Ubuntu installations were not affected. Original advisory details: Tavis Ormandy discovered multiple flaws in the GNU C Library's handling of the `LD_AUDIT` environment variable when running a privileged binary. A local attacker could exploit this to gain root privileges. (CVE-2010-3847, CVE-2010-3856) The problem can be corrected by updating your system to the following package version: To update your system, please follow these instructions: <https://wiki.ubuntu.com/Security/Upgrades>. In general, a standard system update will make all the necessary changes. LP: 701783

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libc6 2.7-10ubuntu5

References:

Source	Reference
USN	USN-1009-2

Vulnerability Solution:

- libc6 on Ubuntu Linux 10.04
Upgrade libc6 for Ubuntu 10.04 LTS
Use ``apt-get upgrade`` to upgrade libc6 to the latest version
- libc6 on Ubuntu Linux 10.10
Upgrade libc6 for Ubuntu 10.10
Use ``apt-get upgrade`` to upgrade libc6 to the latest version
- libc6 on Ubuntu Linux 8.04
Upgrade libc6 for Ubuntu 8.04 LTS
Use ``apt-get upgrade`` to upgrade libc6 to the latest version
- libc6 on Ubuntu Linux 9.10
Upgrade libc6 for Ubuntu 9.10
Use ``apt-get upgrade`` to upgrade libc6 to the latest version

3.2.201. USN-1016-1: libxml2 vulnerability (ubuntu-usn-1016-1)*Description:*

libxml2 before 2.7.8, as used in Google Chrome before 7.0.517.44, Apple Safari 5.0.2 and earlier, and other products, reads from invalid memory locations during processing of malformed XPath expressions, which allows context-dependent attackers to cause a denial of service (application crash) via a crafted XML document.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libxml2 2.6.31.dfsg-2ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2010-11-22-1
APPLE	APPLE-SA-2011-03-02-1
APPLE	APPLE-SA-2011-03-09-2
APPLE	APPLE-SA-2011-03-21-1
BID	44779
CVE	CVE-2010-4008
DEBIAN	DSA-2128
DISA_SEVERITY	Category I
DISA_VMSKEY	V0032171
DISA_VMSKEY	V0033884
IAVM	2012-A-0073
IAVM	2012-A-0153
OVAL	OVAL12148
REDHAT	RHSA-2011:1749
REDHAT	RHSA-2013:0217
USN	USN-1016-1

Vulnerability Solution:

- libxml2 on Ubuntu Linux 10.04
Upgrade libxml2 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libxml2 to the latest version
- libxml2 on Ubuntu Linux 10.10
Upgrade libxml2 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libxml2 to the latest version
- libxml2 on Ubuntu Linux 8.04
Upgrade libxml2 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libxml2 to the latest version

- libxml2 on Ubuntu Linux 9.10

Upgrade libxml2 for Ubuntu 9.10

Use `apt-get upgrade` to upgrade libxml2 to the latest version

3.2.202. USN-1134-1: APR vulnerabilities (ubuntu-usn-1134-1)

Description:

The fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library 1.4.3 and 1.4.4, and the Apache HTTP Server 2.2.18, allows remote attackers to cause a denial of service (infinite loop) via a URI that does not match unspecified types of wildcard patterns, as demonstrated by attacks against mod_autoindex in httpd when a /*/WEB-INF/ configuration pattern is used.

NOTE: this issue exists because of an incorrect fix for CVE-2011-0419.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libapr1 1.2.11-1

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
CVE	CVE-2011-0419
CVE	CVE-2011-1928
DEBIAN	DSA-2237
DISA_SEVERITY	Category II
DISA_VMSKEY	V0027639
IAVM	2011-B-0060
OVAL	OVAL14638
OVAL	OVAL14804
REDHAT	RHSA-2011:0507
REDHAT	RHSA-2011:0844
REDHAT	RHSA-2011:0896
REDHAT	RHSA-2011:0897
USN	USN-1134-1

Vulnerability Solution:

- libapr1 on Ubuntu Linux 10.04

Upgrade libapr1 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libapr1 to the latest version

- libapr1 on Ubuntu Linux 10.10

Upgrade libapr1 for Ubuntu 10.10

Use `apt-get upgrade` to upgrade libapr1 to the latest version

- libapr1 on Ubuntu Linux 11.04

Upgrade libapr1 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade libapr1 to the latest version

- libapr1 on Ubuntu Linux 8.04

Upgrade libapr1 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libapr1 to the latest version

3.2.203. USN-1215-1: APT vulnerabilities (ubuntu-usn-1215-1)

Description:

It was discovered that the apt-key utility incorrectly verified GPGkeys 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. The problem can be corrected by updating your system to the following package version: To update your system, please follow these instructions: <https://wiki.ubuntu.com/Security/Upgrades>. In general, a standard system update will make all the necessary changes. LP: 856489

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu apt 0.7.9ubuntu17

References:

Source	Reference
USN	USN-1215-1

Vulnerability Solution:

- apt on Ubuntu Linux 10.04

Upgrade apt for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade apt to the latest version

- apt on Ubuntu Linux 10.10

Upgrade apt for Ubuntu 10.10

Use `apt-get upgrade` to upgrade apt to the latest version

- apt on Ubuntu Linux 11.04

Upgrade apt for Ubuntu 11.04

Use `apt-get upgrade` to upgrade apt to the latest version

- apt on Ubuntu Linux 8.04

Upgrade apt for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade apt to the latest version

3.2.204. USN-1427-1: MySQL vulnerabilities (ubuntu-usn-1427-1)

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 5.1.62 in Ubuntu 10.04 LTS, Ubuntu 11.04 and Ubuntu 11.10. Ubuntu 8.04 LTS has been updated to MySQL 5.0.96. 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-5-1-62.html> <http://dev.mysql.com/doc/refman/5.0/en/news-5-0-96.html> The problem can be corrected by updating your system to the following package version: To update your system, please follow these instructions: <https://wiki.ubuntu.com/Security/Upgrades>. In general, a standard system update will make all the necessary changes. LP: 965523

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu mysql-server-5.0 5.0.51a-3ubuntu5

References:

Source	Reference
USN	USN-1427-1

Vulnerability Solution:

- mysql-server-5.0 on Ubuntu Linux 8.04

Upgrade mysql-server-5.0 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade mysql-server-5.0 to the latest version

- mysql-server-5.1 on Ubuntu Linux 10.04

Upgrade mysql-server-5.1 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade mysql-server-5.1 to the latest version

- mysql-server-5.1 on Ubuntu Linux 11.04

Upgrade mysql-server-5.1 for Ubuntu 11.04

Use `apt-get upgrade` to upgrade mysql-server-5.1 to the latest version

- mysql-server-5.1 on Ubuntu Linux 11.10

Upgrade mysql-server-5.1 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade mysql-server-5.1 to the latest version

3.2.205. USN-1450-1: Net-SNMP vulnerability (ubuntu-usn-1450-1)*Description:*

Array index error in the handle_nsExtendOutput2Table function in agent/mibgroup/agent/extend.c in Net-SNMP 5.7.1 allows remote authenticated users to cause a denial of service (out-of-bounds read and snmpd crash) via an SNMP GET request for an entry not in the extension table.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libsnmp15 5.4.1~dfsg-4ubuntu4.3

References:

Source	Reference
BID	53255
BID	53258
CVE	CVE-2012-2141
REDHAT	RHSA-2013:0124
USN	USN-1450-1
XF	75169

Vulnerability Solution:

- libsnmp15 on Ubuntu Linux 10.04
Upgrade libsnmp15 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libsnmp15 to the latest version
- libsnmp15 on Ubuntu Linux 11.04
Upgrade libsnmp15 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade libsnmp15 to the latest version
- libsnmp15 on Ubuntu Linux 11.10
Upgrade libsnmp15 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade libsnmp15 to the latest version
- libsnmp15 on Ubuntu Linux 12.04
Upgrade libsnmp15 for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade libsnmp15 to the latest version
- libsnmp15 on Ubuntu Linux 8.04
Upgrade libsnmp15 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libsnmp15 to the latest version

3.2.206. USN-1461-1: PostgreSQL vulnerabilities (ubuntu-usn-1461-1)

Description:

The crypt_des (aka DES-based crypt) function in FreeBSD before 9.0-RELEASE-p2, as used in PHP, PostgreSQL, and other products, does not process the complete cleartext password if this password contains a 0x80 character, which makes it easier for context-dependent attackers to obtain access via an authentication attempt with an initial substring of the intended password, as demonstrated by a Unicode password.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu postgresql-8.3 8.3.1-1

References:

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
CVE	CVE-2012-2143
CVE	CVE-2012-2655
DEBIAN	DSA-2491
REDHAT	RHSA-2012:1037
USN	USN-1461-1

Vulnerability Solution:

- postgresql-8.3 on Ubuntu Linux 8.04
Upgrade postgresql-8.3 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version
- postgresql-8.4 on Ubuntu Linux 10.04
Upgrade postgresql-8.4 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version
- postgresql-8.4 on Ubuntu Linux 11.04
Upgrade postgresql-8.4 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version
- postgresql-9.1 on Ubuntu Linux 11.10
Upgrade postgresql-9.1 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade postgresql-9.1 to the latest version
- postgresql-9.1 on Ubuntu Linux 12.04
Upgrade postgresql-9.1 for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade postgresql-9.1 to the latest version

3.2.207. USN-1570-1: GnuPG vulnerability (ubuntu-usn-1570-1)*Description:*

It was discovered that GnuPG used a short ID when downloading keys from akeyserver, even if a long ID was requested. An attacker could possibly use this to return a different key with a duplicate short key id. The problem can be corrected by updating your system to the following package version: To update your system, please follow these instructions: <https://wiki.ubuntu.com/Security/Upgrades>. In general, a standard system update will make all the necessary changes. LP: 1016643

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu gnupg 1.4.6-2ubuntu5

References:

Source	Reference
USN	USN-1570-1

Vulnerability Solution:

- gnupg on Ubuntu Linux 10.04
Upgrade gnupg for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade gnupg to the latest version
- gnupg on Ubuntu Linux 11.04
Upgrade gnupg for Ubuntu 11.04
Use `apt-get upgrade` to upgrade gnupg to the latest version
- gnupg on Ubuntu Linux 11.10
Upgrade gnupg for Ubuntu 11.10
Use `apt-get upgrade` to upgrade gnupg to the latest version
- gnupg on Ubuntu Linux 12.04
Upgrade gnupg for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade gnupg to the latest version
- gnupg on Ubuntu Linux 8.04
Upgrade gnupg for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade gnupg to the latest version
- gnupg2 on Ubuntu Linux 10.04
Upgrade gnupg2 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade gnupg2 to the latest version
- gnupg2 on Ubuntu Linux 11.04
Upgrade gnupg2 for Ubuntu 11.04
Use `apt-get upgrade` to upgrade gnupg2 to the latest version

- gnupg2 on Ubuntu Linux 11.10
Upgrade gnupg2 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade gnupg2 to the latest version
- gnupg2 on Ubuntu Linux 12.04
Upgrade gnupg2 for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade gnupg2 to the latest version
- gnupg2 on Ubuntu Linux 8.04
Upgrade gnupg2 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade gnupg2 to the latest version

3.2.208. USN-1686-1: FreeType vulnerabilities (ubuntu-usn-1686-1)

Description:

The `_bdf_parse_glyphs` function in FreeType before 2.4.11 allows context-dependent attackers to cause a denial of service (out-of-bounds write and crash) via vectors related to BDF fonts and an `ENCODING` field with a negative value.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libfreetype6 2.3.5-1ubuntu4.8.04.2

References:

Source	Reference
CVE	CVE-2012-5668
CVE	CVE-2012-5669
CVE	CVE-2012-5670
REDHAT	RHSA-2013:0216
USN	USN-1686-1

Vulnerability Solution:

- libfreetype6 on Ubuntu Linux 10.04
Upgrade libfreetype6 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libfreetype6 to the latest version
- libfreetype6 on Ubuntu Linux 11.10
Upgrade libfreetype6 for Ubuntu 11.10
Use `apt-get upgrade` to upgrade libfreetype6 to the latest version
- libfreetype6 on Ubuntu Linux 12.04
Upgrade libfreetype6 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

- libfreetype6 on Ubuntu Linux 12.10

Upgrade libfreetype6 for Ubuntu 12.10

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

- libfreetype6 on Ubuntu Linux 8.04

Upgrade libfreetype6 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libfreetype6 to the latest version

3.2.209. USN-1752-1: GnuTLS vulnerability (ubuntu-usn-1752-1)

Description:

The TLS implementation in GnuTLS before 2.12.23, 3.0.x before 3.0.28, and 3.1.x before 3.1.7 does not properly consider timing side-channel attacks on a noncompliant MAC check operation during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, a related issue to CVE-2013-0169.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libgnutls13 2.0.4-1ubuntu2

References:

Source	Reference
CVE	CVE-2013-1619
REDHAT	RHSA-2013:0588
USN	USN-1752-1

Vulnerability Solution:

- libgnutls13 on Ubuntu Linux 8.04

Upgrade libgnutls13 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libgnutls13 to the latest version

- libgnutls26 on Ubuntu Linux 10.04

Upgrade libgnutls26 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libgnutls26 to the latest version

- libgnutls26 on Ubuntu Linux 11.10

Upgrade libgnutls26 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libgnutls26 to the latest version

- libgnutls26 on Ubuntu Linux 12.04

Upgrade libgnutls26 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libgnutls26 to the latest version

- libgnutls26 on Ubuntu Linux 12.10

Upgrade libgnutls26 for Ubuntu 12.10

Use `apt-get upgrade` to upgrade libgnutls26 to the latest version

3.2.210. USN-1782-1: libxml2 vulnerability (ubuntu-usn-1782-1)

Description:

libxml2 2.9.0 and earlier allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via an XML file containing an entity declaration with long replacement text and many references to this entity, aka "internal entity expansion" with linear complexity.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu libxml2 2.6.31.dfsg-2ubuntu1

References:

Source	Reference
CVE	CVE-2013-0338
DEBIAN	DSA-2652
USN	USN-1782-1

Vulnerability Solution:

- libxml2 on Ubuntu Linux 10.04

Upgrade libxml2 for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version
- libxml2 on Ubuntu Linux 11.10

Upgrade libxml2 for Ubuntu 11.10

Use `apt-get upgrade` to upgrade libxml2 to the latest version
- libxml2 on Ubuntu Linux 12.04

Upgrade libxml2 for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version
- libxml2 on Ubuntu Linux 12.10

Upgrade libxml2 for Ubuntu 12.10

Use `apt-get upgrade` to upgrade libxml2 to the latest version
- libxml2 on Ubuntu Linux 8.04

Upgrade libxml2 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version

3.2.211. USN-640-1: libxml2 vulnerability (ubuntu-usn-640-1)*Description:*

libxml2 2.6.32 and earlier does not properly detect recursion during entity expansion in an attribute value, which allows context-dependent attackers to cause a denial of service (memory and CPU consumption) via a crafted XML document.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libxml2 2.6.31.dfsg-2ubuntu1

References:

Source	Reference
APPLE	APPLE-SA-2009-06-08-1
APPLE	APPLE-SA-2009-06-17-1
BID	30783
CVE	CVE-2008-3281
DEBIAN	DSA-1631
OVAL	OVAL6496
OVAL	OVAL9812
REDHAT	RHSA-2008:0836
USN	USN-640-1

Vulnerability Solution:

•libxml2 on Ubuntu Linux 7.04

Upgrade libxml2 for Ubuntu 7.04

Use `apt-get upgrade` to upgrade libxml2 to the latest version

•libxml2 on Ubuntu Linux 7.10

Upgrade libxml2 for Ubuntu 7.10

Use `apt-get upgrade` to upgrade libxml2 to the latest version

•libxml2 on Ubuntu Linux 8.04

Upgrade libxml2 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libxml2 to the latest version

3.2.212. USN-670-1: VMBuilder vulnerability (ubuntu-usn-670-1)

Description:

Mathias Gug discovered that vm-builder improperly set the rootpassword when creating virtual machines. An attacker could exploit this to gain root privileges to the virtual machine by using a predictable password. This vulnerability only affects virtual machines created with vm-builder under Ubuntu 8.10, and does not affect native Ubuntu installations. An update was made to the shadow package to detect vulnerable systems and disable password authentication for the root account. Vulnerable virtual machines which an attacker has access to should be considered compromised, and appropriate action taken to secure the machine. The problem can be corrected by updating your system to the following package version: To update your system, please follow these instructions: <https://wiki.ubuntu.com/Security/Upgrades>. In general, a standard system upgrade is sufficient to effect the necessary changes. <https://bugs.launchpad.net/+bug/296841>

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu passwd 1:4.0.18.2-1ubuntu2

References:

Source	Reference
USN	USN-670-1

Vulnerability Solution:

- passwd on Ubuntu Linux 7.10
Upgrade passwd for Ubuntu 7.10
Use `apt-get upgrade` to upgrade passwd to the latest version
- passwd on Ubuntu Linux 8.04
Upgrade passwd for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade passwd to the latest version
- passwd on Ubuntu Linux 8.10
Upgrade passwd for Ubuntu 8.10
Use `apt-get upgrade` to upgrade passwd to the latest version
- python-vm-builder on Ubuntu Linux 8.10
Upgrade python-vm-builder for Ubuntu 8.10
Use `apt-get upgrade` to upgrade python-vm-builder to the latest version

3.2.213. USN-678-1: GnuTLS vulnerability (ubuntu-usn-678-1)*Description:*

The `_gnutls_x509_verify_certificate` function in `lib/x509/verify.c` in `libgnutls` in GnuTLS before 2.6.1 trusts certificate chains in which the last certificate is an arbitrary trusted, self-signed certificate, which allows man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libgnutls13 2.0.4-1ubuntu2

References:

Source	Reference
BID	32232
CVE	CVE-2008-4989
DEBIAN	DSA-1719
OVAL	OVAL11650
REDHAT	RHSA-2008:0982
USN	USN-678-1
XF	46482

Vulnerability Solution:

- libgnutls13 on Ubuntu Linux 7.10
Upgrade libgnutls13 for Ubuntu 7.10
Use `apt-get upgrade` to upgrade libgnutls13 to the latest version
- libgnutls13 on Ubuntu Linux 8.04
Upgrade libgnutls13 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libgnutls13 to the latest version
- libgnutls26 on Ubuntu Linux 8.10
Upgrade libgnutls26 for Ubuntu 8.10
Use `apt-get upgrade` to upgrade libgnutls26 to the latest version

3.2.214. USN-753-1: PostgreSQL vulnerability (ubuntu-usn-753-1)*Description:*

PostgreSQL before 8.3.7, 8.2.13, 8.1.17, 8.0.21, and 7.4.25 allows remote authenticated users to cause a denial of service (stack consumption and crash) by triggering a failure in the conversion of a localized error message to a client-specified encoding, as demonstrated using mismatched encoding conversion requests.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu postgresql-8.3 8.3.1-1

References:

Source	Reference
BID	34090
CVE	CVE-2009-0922
OVAL	OVAL10874
OVAL	OVAL6252
REDHAT	RHSA-2009:1067
USN	USN-753-1

Vulnerability Solution:

- postgresql-8.3 on Ubuntu Linux 8.04
Upgrade postgresql-8.3 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version
- postgresql-8.3 on Ubuntu Linux 8.10
Upgrade postgresql-8.3 for Ubuntu 8.10
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version

3.2.215. USN-799-1: D-Bus vulnerability (ubuntu-usn-799-1)*Description:*

The `_dbus_validate_signature_with_reason` function (`dbus-marshal-validate.c`) in D-Bus (aka DBus) before 1.2.14 uses incorrect logic to validate a basic type, which allows remote attackers to spoof a signature via a crafted key. NOTE: this is due to an incorrect fix for CVE-2008-3834.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libdbus-1-3 1.1.20-1ubuntu1

References:

Source	Reference
BID	31602

Source	Reference
CVE	CVE-2009-1189
OVAL	OVAL10308
REDHAT	RHSA-2010:0095
USN	USN-799-1
XF	50385

Vulnerability Solution:

•libdbus-1-3 on Ubuntu Linux 8.04

Upgrade libdbus-1-3 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version

•libdbus-1-3 on Ubuntu Linux 8.10

Upgrade libdbus-1-3 for Ubuntu 8.10

Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version

•libdbus-1-3 on Ubuntu Linux 9.04

Upgrade libdbus-1-3 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version

3.2.216. USN-808-1: Bind vulnerability (ubuntu-usn-808-1)*Description:*

The dns_db_findrdataset function in db.c in named in ISC BIND 9.4 before 9.4.3-P3, 9.5 before 9.5.1-P3, and 9.6 before 9.6.1-P1, when configured as a master server, allows remote attackers to cause a denial of service (assertion failure and daemon exit) via an ANY record in the prerequisite section of a crafted dynamic update message, as exploited in the wild in July 2009.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu bind9 1:9.4.2-10

References:

Source	Reference
CERT-VN	725188
CVE	CVE-2009-0696
NETBSD	NetBSD-SA2009-013
OVAL	OVAL10414
OVAL	OVAL12245

Source	Reference
OVAL	OVAL7806
USN	USN-808-1

Vulnerability Solution:

•bind9 on Ubuntu Linux 8.04

Upgrade bind9 for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade bind9 to the latest version

•bind9 on Ubuntu Linux 8.10

Upgrade bind9 for Ubuntu 8.10

Use `apt-get upgrade` to upgrade bind9 to the latest version

•bind9 on Ubuntu Linux 9.04

Upgrade bind9 for Ubuntu 9.04

Use `apt-get upgrade` to upgrade bind9 to the latest version

3.2.217. USN-855-1: libhtml-parser-perl vulnerability (ubuntu-usn-855-1)*Description:*

The decode_entities function in util.c in HTML-Parser before 3.63 allows context-dependent attackers to cause a denial of service (infinite loop) via an incomplete SGML numeric character reference, which triggers generation of an invalid UTF-8 character.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libhtml-parser-perl 3.56-1

References:

Source	Reference
BID	36807
CVE	CVE-2009-3627
USN	USN-855-1
XF	53941

Vulnerability Solution:

•libhtml-parser-perl on Ubuntu Linux 8.04

Upgrade libhtml-parser-perl for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade libhtml-parser-perl to the latest version

•libhtml-parser-perl on Ubuntu Linux 8.10

Upgrade libhtml-parser-perl for Ubuntu 8.10

Use `apt-get upgrade` to upgrade libhtml-parser-perl to the latest version

- libhtml-parser-perl on Ubuntu Linux 9.04

Upgrade libhtml-parser-perl for Ubuntu 9.04

Use `apt-get upgrade` to upgrade libhtml-parser-perl to the latest version

- libhtml-parser-perl on Ubuntu Linux 9.10

Upgrade libhtml-parser-perl for Ubuntu 9.10

Use `apt-get upgrade` to upgrade libhtml-parser-perl to the latest version

3.2.218. USN-918-1: Samba vulnerability (ubuntu-usn-918-1)

Description:

The default configuration of smbd in Samba before 3.3.11, 3.4.x before 3.4.6, and 3.5.x before 3.5.0rc3, when a writable share exists, allows remote authenticated users to leverage a directory traversal vulnerability, and access arbitrary files, by using the symlink command in smbclient to create a symlink containing .. (dot dot) sequences, related to the combination of the unix extensions and wide links options.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu samba 3.0.20-0.1ubuntu1

References:

Source	Reference
CVE	CVE-2010-0926
USN	USN-918-1

Vulnerability Solution:

- samba on Ubuntu Linux 8.04

Upgrade samba for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade samba to the latest version

- samba on Ubuntu Linux 8.10

Upgrade samba for Ubuntu 8.10

Use `apt-get upgrade` to upgrade samba to the latest version

- samba on Ubuntu Linux 9.04

Upgrade samba for Ubuntu 9.04

Use `apt-get upgrade` to upgrade samba to the latest version

- samba on Ubuntu Linux 9.10

Upgrade samba for Ubuntu 9.10

Use `apt-get upgrade` to upgrade samba to the latest version

3.2.219. USN-928-1: Sudo vulnerability (ubuntu-usn-928-1)*Description:*

Valerio Costamagna discovered that sudo did not properly validate the path for the 'sudoedit' pseudo-command when the PATH contained only a dot ('.'). If secure_path and ignore_dot were disabled, a local attacker could exploit this to execute arbitrary code as root if sudo was configured to allow the attacker to use sudoedit. By default, secure_path is used and the sudoedit pseudo-command is not used in Ubuntu. This is a different but related issue to CVE-2010-0426. The problem can be corrected by updating your system to the following package version: To update your system, please follow these instructions: <https://wiki.ubuntu.com/Security/Upgrades>. In general, a standard system upgrade is sufficient to effect the necessary changes. LP: 563963

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu sudo 1.6.9p10-1ubuntu3

References:

Source	Reference
USN	USN-928-1

Vulnerability Solution:

- sudo on Ubuntu Linux 8.04
Upgrade sudo for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo on Ubuntu Linux 8.10
Upgrade sudo for Ubuntu 8.10
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo on Ubuntu Linux 9.04
Upgrade sudo for Ubuntu 9.04
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo on Ubuntu Linux 9.10
Upgrade sudo for Ubuntu 9.10
Use `apt-get upgrade` to upgrade sudo to the latest version
- sudo-ldap on Ubuntu Linux 8.04
Upgrade sudo-ldap for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade sudo-ldap to the latest version
- sudo-ldap on Ubuntu Linux 8.10
Upgrade sudo-ldap for Ubuntu 8.10
Use `apt-get upgrade` to upgrade sudo-ldap to the latest version

- sudo-lldap on Ubuntu Linux 9.04

Upgrade sudo-lldap for Ubuntu 9.04

Use `apt-get upgrade` to upgrade sudo-lldap to the latest version

- sudo-lldap on Ubuntu Linux 9.10

Upgrade sudo-lldap for Ubuntu 9.10

Use `apt-get upgrade` to upgrade sudo-lldap to the latest version

3.2.220. Non-absolute directory entries in PATH (unix-dot-entries-in-root-path)

Description:

Non-absolute (ie. relative) directory entries (such as "." or ".." or "subdir1/subdir2") have been found in the PATH variable. An attacker could elevate his privileges by creating strategically named executable files (such as "ls") and waiting for a user to execute a command with the same name from a particular current working directory (CWD).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	User "stdin" has the following unwanted entries in his/her PATH: is not a tty

References:

None

Vulnerability Solution:

Remove any non-absolute directory entries from the PATH variable. Depending on the configuration and type of operating system, this variable may be defined or modified in one of the following system or user files:

- /etc/environment
- /etc/profile
- /etc/rc
- /etc/login.defs
- /etc/csh.*
- /etc/ksh.*
- /etc/bash.*
- ~/.profile
- ~/.login
- ~/.shrc

3.2.221. Root's umask value is unsafe (unix-umask-unsafe)

Description:

The umask value for root was found to be unsafe. The umask value determines the file permission for newly created files. It specifies the permissions which should not be given by default to the newly created file. Although the default value of umask in most unix

systems is 022, it is a common practice to set it to 077 to be safe.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	The umask value was found to be 0022 but was expected to be 0077

References:

None

Vulnerability Solution:

To ensure complete access control over newly created files, set the umask value to 077 for root and other user accounts for both interactive and non-interactive processes. The umask value for interactive processes is typically set in a shell configuration file such as .login, .cshrc, .profile, .bashrc, .bash_profile, or others. For non-interactive processes, /etc/login.defs is a common location for controlling umask on Linux systems. In both cases, you may need to consult your operating system's documentation for the correct file(s) and settings.

3.2.222. World writable files exist (unix-world-writable-files)

Description:

World writable files were found on the system. A file that can be written by any user on the system could be a serious security flaw.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	<p>The following world writable files were found.</p> <ul style="list-style-type: none"> /var/www/twiki/data/Sandbox/WebChanges.txt /var/www/twiki/data/Sandbox/.mailnotify /var/www/twiki/data/Sandbox/WebHome.txt /var/www/twiki/data/Sandbox/WebNotify.txt /var/www/twiki/data/Sandbox/WebTopicList.txt /var/www/twiki/data/Sandbox/WebChanges.txt,v /var/www/twiki/data/Sandbox/WebNotify.txt,v /var/www/twiki/data/Sandbox/WebSearch.txt /var/www/twiki/data/Sandbox/WebIndex.txt,v /var/www/twiki/data/Sandbox/WebPreferences.txt /var/www/twiki/data/Sandbox/WebHome.txt,v /var/www/twiki/data/Sandbox/WebTopicList.txt,v /var/www/twiki/data/Sandbox/WebSearch.txt,v /var/www/twiki/data/Sandbox/WebStatistics.txt /var/www/twiki/data/Sandbox/WebPreferences.txt,v /var/www/twiki/data/Sandbox/.changes /var/www/twiki/data/Sandbox/WebIndex.txt /var/www/twiki/data/Sandbox/WebStatistics.txt,v

Affected Nodes:	Additional Information:
	/var/www/twiki/data/Main/WebRss.txt/var/www/twiki/data/Main/WebChanges.txt /var/www/twiki/data/Main/AndreaSterbini.txt,v /var/www/twiki/data/Main/NobodyGroup.txt/var/www/twiki/data/Main/.mailnotify /var/www/twiki/data/Main/AndreaSterbini.txt /var/www/twiki/data/Main/LondonOffice.txt,v /var/www/twiki/data/Main/FileAttachment.txt /var/www/twiki/data/Main/TWikiVariables.txt /var/www/twiki/data/Main/TWikiGuest.txt,v /var/www/twiki/data/Main/WebHome.txt/var/www/twiki/data/Main/NicholasLee.txt /var/www/twiki/data/Main/SanJoseOffice.txt,v /var/www/twiki/data/Main/WebNotify.txt/var/www/twiki/data/Main/GrantBow.txt /var/www/twiki/data/Main/WebTopicList.txt /var/www/twiki/data/Main/OfficeLocations.txt,v /var/www/twiki/data/Main/WebRss.txt,v /var/www/twiki/data/Main/MikeMannix.txt,v /var/www/twiki/data/Main/JohnTalintyre.txt /var/www/twiki/data/Main/KevinKinnell.txt /var/www/twiki/data/Main/OfficeLocations.txt /var/www/twiki/data/Main/LondonOffice.txt /var/www/twiki/data/Main/TWikiGroups.txt /var/www/twiki/data/Main/PeterThoeny.txt /var/www/twiki/data/Main/PeterThoeny.txt,v /var/www/twiki/data/Main/WebChanges.txt,v /var/www/twiki/data/Main/TokyoOffice.txt /var/www/twiki/data/Main/WebNotify.txt,v /var/www/twiki/data/Main/GrantBow.txt,v /var/www/twiki/data/Main/WebSearch.txt /var/www/twiki/data/Main/FileAttachment.txt,v

References:

None

Vulnerability Solution:

For each world-writable file, determine whether there is a good reason for it to be world writable. If not, remove world write permissions for the file.

3.3. Moderate Vulnerabilities

3.3.1. Apache HTTPD: CRLF injection in mod_negotiation when untrusted uploads are supported (CVE-2008-0456) (apache-httpd-cve-2008-0456)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_negotiation. Review your web server configuration for validation. Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_negotiation and allow untrusted uploads to locations which have MultiViews enabled.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
APPLE	APPLE-SA-2009-05-12
BID	27409
CERT	TA09-133A
CVE	CVE-2008-0456
REDHAT	RHSA-2013:0130
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	39893

Vulnerability Solution:

Apache HTTPD >= 2.2 and < 2.2.12

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.3.2. ISC BIND: Cache Update From Additional Section (CVE-2009-4022) (dns-bind9-dnssec-cache-poisoning)*Description:*

Unspecified vulnerability in ISC BIND 9.0.x through 9.3.x, 9.4 before 9.4.3-P4, 9.5 before 9.5.2-P1, 9.6 before 9.6.1-P2, and 9.7 beta before 9.7.0b3, with DNSSEC validation enabled and checking disabled (CD), allows remote attackers to conduct DNS cache poisoning attacks by receiving a recursive client query and sending a response that contains an Additional section with crafted data, which is not properly handled when the response is processed "at the same time as requesting DNSSEC records (DO)," aka Bug 20438.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.0.102:53	Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	37118
CERT-VN	418861
CVE	CVE-2009-4022
OSVDB	60493
OVAL	OVAL10821
OVAL	OVAL11745
OVAL	OVAL7261
OVAL	OVAL7459
REDHAT	RHSA-2009:1620
URL	https://kb.isc.org/article/AA-00931/0
URL	https://kb.isc.org/article/AA-00931/187/CVE-2009-4022%3A-BIND-9-Cache-Update-from-Additional-Section.html
XF	54416

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the [ISC website](#).

3.3.3. Oracle MySQL Vulnerability: CVE-2012-0114 (oracle-mysql-cve-2012-0114)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows local users to affect confidentiality and integrity via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0114
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

- Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.3.4. PHP Vulnerability: CVE-2014-3981 (php-cve-2014-3981)*Description:*

acinclude.m4, as used in the configure script in PHP 5.5.13 and earlier, allows local users to overwrite arbitrary files via a symlink attack on the /tmp/phpglibccheck file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
CVE	CVE-2014-3981

Vulnerability Solution:

- Upgrade to PHP version 5.4.30

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 5.5.14

Download and apply the upgrade from: <http://www.php.net/releases/>

3.3.5. USN-1077-1: FUSE vulnerabilities (ubuntu-usn-1077-1)

Description:

Certain legacy functionality in fusermount in fuse 2.8.5 and earlier, when util-linux does not support the --no-canonicalize option, allows local users to bypass intended access restrictions and unmount arbitrary directories via a symlink attack.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu fuse-utils 2.7.2-1ubuntu2

References:

Source	Reference
CVE	CVE-2011-0541
CVE	CVE-2011-0542
CVE	CVE-2011-0543
USN	USN-1077-1

Vulnerability Solution:

•fuse-utils on Ubuntu Linux 10.04

Upgrade fuse-utils for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade fuse-utils to the latest version

•fuse-utils on Ubuntu Linux 10.10

Upgrade fuse-utils for Ubuntu 10.10

Use `apt-get upgrade` to upgrade fuse-utils to the latest version

•fuse-utils on Ubuntu Linux 8.04

Upgrade fuse-utils for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade fuse-utils to the latest version

•fuse-utils on Ubuntu Linux 9.10

Upgrade fuse-utils for Ubuntu 9.10

Use `apt-get upgrade` to upgrade fuse-utils to the latest version

3.3.6. USN-1283-1: APT vulnerability (ubuntu-usn-1283-1)

Description:

methods/https.cc in apt before 0.8.11 accepts connections when the certificate host name fails validation and Verify-Host is enabled, which allows man-in-the-middle attackers to obtain repository credentials via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu apt 0.7.9ubuntu17

References:

Source	Reference
CVE	CVE-2011-3634
USN	USN-1283-1

Vulnerability Solution:

- apt on Ubuntu Linux 10.04
Upgrade apt for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade apt to the latest version
- apt on Ubuntu Linux 10.10
Upgrade apt for Ubuntu 10.10
Use `apt-get upgrade` to upgrade apt to the latest version
- apt on Ubuntu Linux 11.04
Upgrade apt for Ubuntu 11.04
Use `apt-get upgrade` to upgrade apt to the latest version
- apt on Ubuntu Linux 8.04
Upgrade apt for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade apt to the latest version

3.3.7. USN-1477-1: APT vulnerability (ubuntu-usn-1477-1)*Description:*

APT 0.7.x before 0.7.25 and 0.8.x before 0.8.16, when using the apt-key net-update to import keyrings, relies on GnuPG argument order and does not check GPG subkeys, which might allow remote attackers to install altered packages via a man-in-the-middle (MITM) attack. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-3587.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu apt 0.7.9ubuntu17

References:

Source	Reference
BID	54046
CVE	CVE-2012-0954
USN	USN-1477-1

Vulnerability Solution:

•apt on Ubuntu Linux 10.04

Upgrade apt for Ubuntu 10.04 LTS

Use `apt-get upgrade` to upgrade apt to the latest version

•apt on Ubuntu Linux 11.04

Upgrade apt for Ubuntu 11.04

Use `apt-get upgrade` to upgrade apt to the latest version

•apt on Ubuntu Linux 11.10

Upgrade apt for Ubuntu 11.10

Use `apt-get upgrade` to upgrade apt to the latest version

•apt on Ubuntu Linux 12.04

Upgrade apt for Ubuntu 12.04 LTS

Use `apt-get upgrade` to upgrade apt to the latest version

•apt on Ubuntu Linux 8.04

Upgrade apt for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade apt to the latest version

3.3.8. USN-1627-1: Apache HTTP Server vulnerabilities (ubuntu-usn-1627-1)*Description:*

The TLS protocol 1.2 and earlier, as used in Mozilla Firefox, Google Chrome, Qt, and other products, can encrypt compressed data without properly obfuscating the length of the unencrypted data, which allows man-in-the-middle attackers to obtain plaintext HTTP headers by observing length differences during a series of guesses in which a string in an HTTP request potentially matches an unknown string in an HTTP header, aka a "CRIME" attack.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu apache2.2-common 2.2.8-1ubuntu0.15

References:

Source	Reference
--------	-----------

Source	Reference
APPLE	APPLE-SA-2013-06-04-1
APPLE	APPLE-SA-2013-09-12-1
BID	55131
BID	55704
CVE	CVE-2012-2687
CVE	CVE-2012-4929
DEBIAN	DSA-2579
DEBIAN	DSA-2627
OVAL	OVAL18832
OVAL	OVAL18920
OVAL	OVAL19539
REDHAT	RHSA-2012:1591
REDHAT	RHSA-2012:1592
REDHAT	RHSA-2012:1594
REDHAT	RHSA-2013:0130
REDHAT	RHSA-2013:0587
USN	USN-1627-1

Vulnerability Solution:

- apache2.2-common on Ubuntu Linux 10.04
Upgrade apache2.2-common for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade apache2.2-common to the latest version
- apache2.2-common on Ubuntu Linux 11.10
Upgrade apache2.2-common for Ubuntu 11.10
Use `apt-get upgrade` to upgrade apache2.2-common to the latest version
- apache2.2-common on Ubuntu Linux 12.04
Upgrade apache2.2-common for Ubuntu 12.04 LTS
Use `apt-get upgrade` to upgrade apache2.2-common to the latest version
- apache2.2-common on Ubuntu Linux 12.10
Upgrade apache2.2-common for Ubuntu 12.10
Use `apt-get upgrade` to upgrade apache2.2-common to the latest version
- apache2.2-common on Ubuntu Linux 8.04
Upgrade apache2.2-common for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade apache2.2-common to the latest version

3.3.9. USN-892-1: FUSE vulnerability (ubuntu-usn-892-1)

Description:

fusermount in FUSE before 2.7.5, and 2.8.x before 2.8.2, allows local users to unmount an arbitrary FUSE filesystem share via a symlink attack on a mountpoint.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04
	Vulnerable software installed: Ubuntu fuse-utils 2.7.2-1ubuntu2

References:

Source	Reference
BID	37983
CVE	CVE-2009-3297
CVE	CVE-2010-0789
DEBIAN	DSA-1989
USN	USN-892-1
XF	55945

Vulnerability Solution:

•fuse-utils on Ubuntu Linux 8.04

Upgrade fuse-utils for Ubuntu 8.04 LTS

Use `apt-get upgrade` to upgrade fuse-utils to the latest version

•fuse-utils on Ubuntu Linux 8.10

Upgrade fuse-utils for Ubuntu 8.10

Use `apt-get upgrade` to upgrade fuse-utils to the latest version

•fuse-utils on Ubuntu Linux 9.04

Upgrade fuse-utils for Ubuntu 9.04

Use `apt-get upgrade` to upgrade fuse-utils to the latest version

•fuse-utils on Ubuntu Linux 9.10

Upgrade fuse-utils for Ubuntu 9.10

Use `apt-get upgrade` to upgrade fuse-utils to the latest version

3.3.10. Oracle MySQL Vulnerability: CVE-2012-0075 (oracle-mysql-cve-2012-0075)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows remote authenticated users to affect integrity via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
BID	51526
CVE	CVE-2012-0075
OSVDB	78374
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72539

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.3.11. Oracle MySQL Vulnerability: CVE-2012-0492 (oracle-mysql-cve-2012-0492)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, and CVE-2012-0485.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
BID	51516
CVE	CVE-2012-0492
OSVDB	78393
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72537

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.3.12. Oracle MySQL Vulnerability: CVE-2012-0493 (oracle-mysql-cve-2012-0493)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0491, and CVE-2012-0495.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0493
OSVDB	78394
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72538

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.3.13. Oracle MySQL Vulnerability: CVE-2012-0494 (oracle-mysql-cve-2012-0494)*Description:*

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows local users to affect availability via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0494
OSVDB	78375
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72540

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

Download and apply the upgrade from: <http://downloads.mysql.com/archives.php>

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.3.14. PHP Vulnerability: CVE-2007-6039 (php-cve-2007-6039)*Description:*

PHP 5.2.5 and earlier allows context-dependent attackers to cause a denial of service (application crash) via a long string in (1) the domain parameter to the dgettext function, the message parameter to the (2) dcgettext or (3) gettext function, the msgid1 parameter to the (4) dngettext or (5) ngettext function, or (6) the classname parameter to the stream_wrapper_register function. NOTE: this might not be a vulnerability in most web server environments that support multiple threads, unless this issue can be demonstrated for code execution.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
BID	26426
BID	26428
CVE	CVE-2007-6039
XF	38442
XF	38443

Vulnerability Solution:

Download and apply the upgrade from: <http://museum.php.net/php5/php-5.2.6.tar.gz>

3.3.15. Postfix vulnerability (CVE-2008-2937) (postfix-cve-2008-2937)*Description:*

Postfix 2.5 before 2.5.4 and 2.6 before 2.6-20080814 delivers to a mailbox file even when this file is not owned by the recipient, which allows local users to read e-mail messages by creating a mailbox file corresponding to another user's account name.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:25	Running SMTP serviceProduct Postfix exists -- Postfix 2.5.1 Vulnerable version of product Postfix found -- Postfix 2.5.1

References:

Source	Reference
BID	30691
CVE	CVE-2008-2937
REDHAT	RHSA-2011:0422
SUSE	SUSE-SA:2008:040
XF	44461

Vulnerability Solution:

For more information or to download Postfix updates, visit the [Postfix website](#).

3.3.16. USN-1044-1: D-Bus vulnerability (ubuntu-usn-1044-1)

Description:

Stack consumption vulnerability in D-Bus (aka DBus) before 1.4.1 allows local users to cause a denial of service (daemon crash) via a message containing many nested variants.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libdbus-1-3 1.1.20-1ubuntu1

References:

Source	Reference
BID	45377
CVE	CVE-2010-4352
DEBIAN	DSA-2149
USN	USN-1044-1

Vulnerability Solution:

- libdbus-1-3 on Ubuntu Linux 10.04
Upgrade libdbus-1-3 for Ubuntu 10.04 LTS
Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version
- libdbus-1-3 on Ubuntu Linux 10.10
Upgrade libdbus-1-3 for Ubuntu 10.10
Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version
- libdbus-1-3 on Ubuntu Linux 8.04
Upgrade libdbus-1-3 for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version
- libdbus-1-3 on Ubuntu Linux 9.10
Upgrade libdbus-1-3 for Ubuntu 9.10
Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version

3.3.17. USN-642-1: Postfix vulnerability (ubuntu-usn-642-1)

Description:

Postfix 2.4 before 2.4.9, 2.5 before 2.5.5, and 2.6 before 2.6-20080902, when used with the Linux 2.6 kernel, leaks epoll file descriptors during execution of "non-Postfix" commands, which allows local users to cause a denial of service (application slowdown or exit) via a crafted command, as demonstrated by a command in a .forward file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu postfix 2.5.1-2ubuntu1

References:

Source	Reference
BID	30977
CVE	CVE-2008-3889
USN	USN-642-1
XF	44865

Vulnerability Solution:

- postfix on Ubuntu Linux 7.10
Upgrade postfix for Ubuntu 7.10
Use `apt-get upgrade` to upgrade postfix to the latest version
- postfix on Ubuntu Linux 8.04
Upgrade postfix for Ubuntu 8.04 LTS
Use `apt-get upgrade` to upgrade postfix to the latest version

3.3.18. Partition Mounting Weakness (unix-partition-mounting-weakness)*Description:*

One or more of the system's partitions are mounted without certain hardening options enabled. While this is not a definite vulnerability on its own, system security may be improved by employing hardening techniques.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	The following issues were discovered: /boot partition does not have 'nodev' option set. /var/lib/nfs/rpc_pipefs partition does not have 'nodev' option set.

References:

None

Vulnerability Solution:

The specific way to modify the partition mount options varies from system to system. Consult your operating system's manual or mount man page.

3.3.19. User home directory mode unsafe (unix-user-home-dir-mode)

Description:

A user's home directory was found to have permissions mode more than 750. Group or world writable user home directories means that a malicious user may gain complete access over vulnerable user's data and privileges. Also the "read" and "execute" access for others should be disabled.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	The permissions for home directory of user msfadmin was found to be 755 instead of 750.

References:

None

Vulnerability Solution:

Restrict the user home directory mode to at most 750 using the command:
chmod 750 userDir

3.3.20. CIFS Share Readable By Everyone (cifs-share-world-readable)

Description:

A share was found which allows read access by anyone. The impact of this vulnerability depends on the contents of the share.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Successfully read share "tmp" and found the following files:#sqlfeb_1c_0.MYD #sqlfeb_1c_0.MYI#sqlfeb_1c_0.frm.ICE-unix.X11-unix.X0-lock4460.jsvc_up

References:

None

Vulnerability Solution:

Adjust the share permissions to restrict access to only those members of the organization who need the data. It is considered bad practice to grant the "Everyone", "Guest", or "Authenticated Users" groups read or write access to a share.

3.3.21. DNS Traffic Amplification (dns-amplification)

Description:

A Domain Name Server (DNS) amplification attack is a popular form of distributed denial of service (DDoS) that relies on the use of publically accessible open DNS servers to overwhelm a victim system with DNS response traffic.

A Domain Name Server (DNS) Amplification attack is a popular form of Distributed Denial of Service (DDoS), in which attackers use publically accessible open DNS servers to flood a target system with DNS response traffic. The primary technique consists of an attacker sending a DNS name lookup request to an open DNS server with the source address spoofed to be the targets address. When the DNS server sends the DNS record response, it is sent instead to the target. Attackers will typically submit a request for as much zone information as possible to maximize the amplification effect. In most attacks of this type observed by US-CERT, the spoofed queries sent by the attacker are of the type, ANY, which returns all known information about a DNS zone in a single request. Because the size of the response is considerably larger than the request, the attacker is able to increase the amount of traffic directed at the victim. By leveraging a botnet to produce a large number of spoofed DNS queries, an attacker can create an immense amount of traffic with little effort. Additionally, because the responses are legitimate data coming from valid servers, it is extremely difficult to prevent these types of attacks. While the attacks are difficult to stop, network operators can apply several possible mitigation strategies.

While the most common form of this attack that US-CERT has observed involves DNS servers configured to allow unrestricted recursive resolution for any client on the Internet, attacks can also involve authoritative name servers that do not provide recursive resolution. The attack method is similar to open recursive resolvers, but is more difficult to mitigate since even a server configured with best practices can still be used in an attack. In the case of authoritative servers, mitigation should focus on using Response Rate Limiting to restrict the amount of traffic.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:53	Running DNS over UDP

References:

Source	Reference
CERT	TA13-088A
CERT	TA14-017A

Vulnerability Solution:

DNS is often vital to the proper functioning of a network. Restrict access to the DNS service to only trusted assets.

3.3.22. FTP access with ftp account (ftp-generic-0001)

Description:

Many FTP servers support a default account with the user ID "ftp" and password "ftp". It is best practice to remove default accounts, if possible. For accounts required by the system, the default password should be changed.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:21	Running FTP service Successfully authenticated to the FTP service with credentials: uid[ftp] pw[ftp] realm[]

References:

Source	Reference
CVE	CVE-1999-0497

Vulnerability Solution:

Remove or disable the account if it is not critical for the system to function. Otherwise, the password should be changed to a non-default value.

3.3.23. FTP access with anonymous account (ftp-generic-0002)*Description:*

Many FTP servers support a default account with the user ID "anonymous" and password "ftp@". It is best practice to remove default accounts, if possible. For accounts required by the system, the default password should be changed.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:21	Running FTP serviceSuccessfully authenticated to the FTP service with credentials: uid[anonymous] pw[joe@] realm[]

References:

Source	Reference
CVE	CVE-1999-0497

Vulnerability Solution:

Remove or disable the account if it is not critical for the system to function. Otherwise, the password should be changed to a non-default value.

3.3.24. ICMP timestamp response (generic-icmp-timestamp)*Description:*

The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services.

In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Able to determine remote system time.

References:

Source	Reference
CVE	CVE-1999-0524
OSVDB	95
XF	306
XF	322

Vulnerability Solution:

•HP-UX

Disable ICMP timestamp responses on HP/UX

Execute the following command:

```
ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Cisco IOS

Disable ICMP timestamp responses on Cisco IOS

Use ACLs to block ICMP types 13 and 14. For example:

```
deny icmp any any 13
```

```
deny icmp any any 14
```

Note that it is generally preferable to use ACLs that block everything by default and then selectively allow certain types of traffic in. For example, block everything and then only allow ICMP unreachable, ICMP echo reply, ICMP time exceeded, and ICMP source quench:

```
permit icmp any any unreachable
```

```
permit icmp any any echo-reply
```

```
permit icmp any any time-exceeded
```

```
permit icmp any any source-quench
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•SGI Irix

Disable ICMP timestamp responses on SGI Irix

IRIX does not offer a way to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using ipfilterd, and/or block it at any external firewalls.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Linux

Disable ICMP timestamp responses on Linux

Linux offers neither a sysctl nor a /proc/sys/net/ipv4 interface to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using iptables, and/or block it at the firewall. For example:

```
ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
```

```
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

- Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition

Disable ICMP timestamp responses on Windows NT 4

Windows NT 4 does not provide a way to block ICMP packets. Therefore, you should block them at the firewall.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

- OpenBSD

Disable ICMP timestamp responses on OpenBSD

Set the "net.inet.icmp.tstamprepl" sysctl variable to 0.

```
sysctl -w net.inet.icmp.tstamprepl=0
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

- Cisco PIX

Disable ICMP timestamp responses on Cisco PIX

A properly configured PIX firewall should never respond to ICMP packets on its external interface. In PIX Software versions 4.1(6) until 5.2.1, ICMP traffic to the PIX's internal interface is permitted; the PIX cannot be configured to NOT respond. Beginning in PIX Software version 5.2.1, ICMP is still permitted on the internal interface by default, but ICMP responses from its internal interfaces can be disabled with the `icmp` command, as follows, where `<inside>` is the name of the internal interface:

```
icmp deny any 13 <inside>
```

```
icmp deny any 14 <inside>
```

Don't forget to save the configuration when you are finished.

See Cisco's support document [Handling ICMP Pings with the PIX Firewall](#) for more information.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

- Sun Solaris

Disable ICMP timestamp responses on Solaris

Execute the following commands:

```
/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp 0
```

```
/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

- Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server

Disable ICMP timestamp responses on Windows 2000

Use the IPsec filter feature to define and apply an IP filter list that blocks ICMP types 13 and 14. Note that the standard TCP/IP blocking capability under the "Networking and Dialup Connections" control panel is NOT capable of blocking ICMP (only TCP and UDP). The IPsec filter features, while they may seem strictly related to the IPsec standards, will allow you to selectively block these ICMP packets. See <http://support.microsoft.com/kb/313190> for more information.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

- Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003

Disable ICMP timestamp responses on Windows XP/2K3

ICMP timestamp responses can be disabled by deselecting the "allow incoming timestamp request" option in the ICMP configuration panel of Windows Firewall.

1. Go to the Network Connections control panel.
2. Right click on the network adapter and select "properties", or select the internet adapter and select File->Properties.
3. Select the "Advanced" tab.
4. In the Windows Firewall box, select "Settings".
5. Select the "General" tab.
6. Enable the firewall by selecting the "on (recommended)" option.
7. Select the "Advanced" tab.
8. In the ICMP box, select "Settings".
9. Deselect (uncheck) the "Allow incoming timestamp request" option.
10. Select "OK" to exit the ICMP Settings dialog and save the settings.
11. Select "OK" to exit the Windows Firewall dialog and save the settings.
12. Select "OK" to exit the internet adapter dialog.

For more information, see: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true

- Microsoft Windows Vista, Microsoft Windows Vista Home, Basic Edition, Microsoft Windows Vista Home, Basic N Edition, Microsoft Windows Vista Home, Premium Edition, Microsoft Windows Vista Ultimate Edition, Microsoft Windows Vista Enterprise Edition, Microsoft Windows Vista Business Edition, Microsoft Windows Vista Business N Edition, Microsoft Windows Vista Starter Edition, Microsoft Windows Server 2008, Microsoft Windows Server 2008 Standard Edition, Microsoft Windows Server 2008 Enterprise Edition, Microsoft Windows Server 2008 Datacenter Edition, Microsoft Windows Server 2008 HPC Edition, Microsoft Windows Server 2008 Web Edition, Microsoft Windows Server 2008 Storage Edition, Microsoft Windows Small Business Server 2008, Microsoft Windows Essential Business Server 2008

Disable ICMP timestamp responses on Windows Vista/2008

ICMP timestamp responses can be disabled via the netsh command line utility.

1. Go to the Windows Control Panel.
2. Select "Windows Firewall".
3. In the Windows Firewall box, select "Change Settings".

4. Enable the firewall by selecting the "on (recommended)" option.
5. Open a Command Prompt.
6. Enter "netsh firewall set icmpsetting 13 disable"

For more information, see: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true

•Disable ICMP timestamp responses

Disable ICMP timestamp replies for the device. If the device does not support this level of configuration, the easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

3.3.25. TCP timestamp response (generic-tcp-timestamp)

Description:

The remote host responded with a TCP timestamp. The TCP timestamp response can be used to approximate the remote host's uptime, potentially aiding in further attacks. Additionally, some operating systems can be fingerprinted based on the behavior of their TCP timestamps.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Able to determine system boot time.

References:

Source	Reference
URL	http://uptime.netcraft.com
URL	http://www.forensicswiki.org/wiki/TCP_timestamps
URL	http://www.ietf.org/rfc/rfc1323.txt

Vulnerability Solution:

•Cisco

Disable TCP timestamp responses on Cisco

Run the following command to disable TCP timestamps:

```
no ip tcp timestamp
```

•FreeBSD

Disable TCP timestamp responses on FreeBSD

Set the value of net.inet.tcp.rfc1323 to 0 by running the following command:

```
sysctl -w net.inet.tcp.rfc1323=0
```

Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:

```
net.inet.tcp.rfc1323=0
```

- Linux

Disable TCP timestamp responses on Linux

Set the value of net.ipv4.tcp_timestamps to 0 by running the following command:

```
sysctl -w net.ipv4.tcp_timestamps=0
```

Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:

```
net.ipv4.tcp_timestamps=0
```

- OpenBSD

Disable TCP timestamp responses on OpenBSD

Set the value of net.inet.tcp.rfc1323 to 0 by running the following command:

```
sysctl -w net.inet.tcp.rfc1323=0
```

Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:

```
net.inet.tcp.rfc1323=0
```

- Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition, Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows 98SE, Microsoft Windows ME, Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server, Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows XP Tablet PC Edition, Microsoft Windows CE, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003, Microsoft Windows Server 2003 R2, Microsoft Windows Server 2003 R2, Standard Edition, Microsoft Windows Server 2003 R2, Enterprise Edition, Microsoft Windows Server 2003 R2, Datacenter Edition, Microsoft Windows Server 2003 R2, Web Edition, Microsoft Windows Small Business Server 2003 R2, Microsoft Windows Server 2003 R2, Express Edition, Microsoft Windows Server 2003 R2, Workgroup Edition

Disable TCP timestamp responses on Windows versions before Vista

Set the Tcp1323Opts value in the following key to 1:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

•Microsoft Windows Server 2008, Microsoft Windows Server 2008 Standard Edition, Microsoft Windows Server 2008 Enterprise Edition, Microsoft Windows Server 2008 Datacenter Edition, Microsoft Windows Server 2008 HPC Edition, Microsoft Windows Server 2008 Web Edition, Microsoft Windows Server 2008 Storage Edition, Microsoft Windows Small Business Server 2008, Microsoft Windows Essential Business Server 2008, Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 R2, Standard Edition, Microsoft Windows Server 2008 R2, Enterprise Edition, Microsoft Windows Server 2008 R2, Datacenter Edition, Microsoft Windows Server 2008 R2, Web Edition, Microsoft Windows Server 2012, Microsoft Windows Server 2012 Standard Edition, Microsoft Windows Server 2012 Foundation Edition, Microsoft Windows Server 2012 Essentials Edition, Microsoft Windows Server 2012 Datacenter Edition, Microsoft Windows Storage Server 2012, Microsoft Windows Vista, Microsoft Windows Vista Home, Basic Edition, Microsoft Windows Vista Home, Basic N Edition, Microsoft Windows Vista Home, Premium Edition, Microsoft Windows Vista Ultimate Edition, Microsoft Windows Vista Enterprise Edition, Microsoft Windows Vista Business Edition, Microsoft Windows Vista Business N Edition, Microsoft Windows Vista Starter Edition, Microsoft Windows 7, Microsoft Windows 7 Home, Basic Edition, Microsoft Windows 7 Home, Basic N Edition, Microsoft Windows 7 Home, Premium Edition, Microsoft Windows 7 Home, Premium N Edition, Microsoft Windows 7 Ultimate Edition, Microsoft Windows 7 Ultimate N Edition, Microsoft Windows 7 Enterprise Edition, Microsoft Windows 7 Enterprise N Edition, Microsoft Windows 7 Professional Edition, Microsoft Windows 7 Starter Edition, Microsoft Windows 7 Starter N Edition, Microsoft Windows 8, Microsoft Windows 8 Enterprise Edition, Microsoft Windows 8 Professional Edition, Microsoft Windows 8 RT, Microsoft Windows Longhorn Server Beta

Disable TCP timestamp responses on Windows versions since Vista

TCP timestamps cannot be reliably disabled on this OS. If TCP timestamps present enough of a risk, put a firewall capable of blocking TCP timestamp packets in front of the affected assets.

3.3.26. NetBIOS NBSTAT Traffic Amplification (netbios-nbstat-amplification)

Description:

A NetBIOS NBSTAT query will obtain the status from a NetBIOS-speaking endpoint, which will include any names that the endpoint is known to respond to as well as the device's MAC address for that endpoint. A NBSTAT response is roughly 3x the size of the request, and because NetBIOS utilizes UDP, this can be used to conduct traffic amplification attacks against other assets, typically in the form of distributed reflected denial of service (DRDoS) attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:137	Running CIFS Name Service serviceConfiguration item advertised-name-count set to '5' matched

References:

Source	Reference
CERT	TA14-017A

Vulnerability Solution:

NetBIOS can be important to the proper functioning of a Windows network depending on the design. Restrict access to the NetBIOS service to only trusted assets.

3.3.27. OpenSSH "X11UseLocalhost" X11 Forwarding Session Hijacking Vulnerability (ssh-openssh-x11uselocalhost-x11-forwarding-session-hijack)

Description:

OpenSSH before 5.1 sets the SO_REUSEADDR socket option when the X11UseLocalhost configuration setting is disabled, which allows local users on some platforms to hijack the X11 forwarding port via a bind to a single IP address, as demonstrated on the HP-UX platform.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102:22	OpenBSD OpenSSH 4.7p1 on Ubuntu Linux 8.04

References:

Source	Reference
BID	30339
CVE	CVE-2008-3259
XF	43940

Vulnerability Solution:

OpenBSD OpenSSH < 5.1

Download and apply the upgrade from: <ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH>

While you can always [build OpenSSH from source](#), many platforms and distributions provide pre-built binary packages for OpenSSH. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.3.28. UDP IP ID Zero (udp-ipid-zero)

Description:

The remote host responded with a UDP packet whose IP ID was zero. Normally the IP ID should be set to a unique value and is used in the reconstruction of fragmented packets. Generally this behavior is only seen with systems derived from a Linux kernel, which may allow an attacker to fingerprint the target's operating system.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.102	Received UDP packet with IP ID of zero:IPv4 SRC[192.168.0.102] TGT[192.168.0.104] TOS[0] TTL[64] Flags[40] Proto[17] ID[0] FragOff[0] HDR-LENGTH[20] TOTAL-LENGTH[52] CKSUM[47258] UDP SRC-PORT[40809] TGT-PORT[9720] CKSUM[38260] RAW DATA [24]: 3EECE3CA000000010000000000000000 >..... 0000000000000001

References:

None

Vulnerability Solution:

Many vendors do not consider this to be a vulnerability, or a vulnerability worth fixing, so there are no vendor-provided solutions aside from putting a firewall or other filtering device between the target and hostile attackers that is capable of randomizing IP IDs.

4. Discovered Services

4.1. <unknown>

4.1.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	1099	0	
192.168.0.102	tcp	3632	0	
192.168.0.102	tcp	6697	0	
192.168.0.102	tcp	8787	0	
192.168.0.102	tcp	37208	0	

4.2. CIFS

4.2.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	139	4	•Samba 3.0.20-Debian
192.168.0.102	tcp	445	4	•Samba 3.0.20-Debian

4.3. CIFS Name Service

4.3.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	udp	137	1	<ul style="list-style-type: none"> •advertised-name-1: METASPLOITABLE (Computer Name) •advertised-name-2: METASPLOITABLE (Logged-on User) •advertised-name-3: METASPLOITABLE (File Server Service) •advertised-name-4: WORKGROUP (Domain Name) •advertised-name-5: WORKGROUP (Browser Service Elections) •advertised-name-count: 5 •mac-address: 000000000000

4.4. DNS

4.4.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	udp	53	0	<ul style="list-style-type: none"> •BIND 9.4.2 •bind.version: 9.4.2
192.168.0.102	tcp	53	0	<ul style="list-style-type: none"> •BIND 9.4.2 •bind.version: 9.4.2
192.168.0.102	udp	53	2	
192.168.0.102	tcp	53	1	
192.168.0.102	udp	53	1	
192.168.0.102	tcp	53	1	
192.168.0.102	udp	53	1	
192.168.0.102	tcp	53	1	
192.168.0.102	udp	53	1	
192.168.0.102	tcp	53	1	
192.168.0.102	udp	53	1	
192.168.0.102	tcp	53	1	
192.168.0.102	udp	53	1	
192.168.0.102	tcp	53	1	
192.168.0.102	udp	53	1	
192.168.0.102	tcp	53	1	
192.168.0.102	udp	53	1	
192.168.0.102	tcp	53	1	

4.5. FTP

4.5.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	21	2	<ul style="list-style-type: none"> •vsFTPD 2.3.4 •ftp.banner: 220 (vsFTPD 2.3.4) •ftp.plaintext.authentication: true •ftp.supports-starttls: false

4.6. FTPS

4.6.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	2121	0	•ftp.banner: 500 HELO not understood

4.7. HTTP

4.7.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	80	9	<ul style="list-style-type: none"> •Apache HTTPD 2.2.8 •DAV: 2 •PHP: 5.2.4-2ubuntu5.10 •http.banner: Apache/2.2.8 (Ubuntu) DAV/2 •http.banner.server: Apache/2.2.8 (Ubuntu) DAV/2 •http.banner.x-powered-by: PHP/5.2.4-2ubuntu5.10
192.168.0.102	tcp	8180	3	<ul style="list-style-type: none"> •Apache Tomcat •Coyote: 1.1 •http.banner: Apache-Coyote/1.1 •http.banner.server: Apache-Coyote/1.1

4.8. MySQL

4.8.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	3306	8	<ul style="list-style-type: none"> •Oracle MySQL 5.0.51a •auto_increment_increment: 1 •auto_increment_offset: 1 •automatic_sp_privileges: ON •back_log: 50 •basedir: /usr/ •binlog_cache_size: 32768 •bulk_insert_buffer_size: 8388608 •character_set_client: latin1 •character_set_connection: latin1 •character_set_database: latin1 •character_set_filesystem: binary

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •character_set_results: •character_set_server: latin1 •character_set_system: utf8 •character_sets_dir: /usr/share/mysql/charsets/ •collation_connection: latin1_swedish_ci •collation_database: latin1_swedish_ci •collation_server: latin1_swedish_ci •completion_type: 0 •concurrent_insert: 1 •connect_timeout: 5 •datadir: /var/lib/mysql/ •date_format: %Y-%m-%d •datetime_format: %Y-%m-%d %H:%i:%s •default_week_format: 0 •delay_key_write: ON •delayed_insert_limit: 100 •delayed_insert_timeout: 300 •delayed_queue_size: 1000 •div_precision_increment: 4 •engine_condition_pushdown: OFF •expire_logs_days: 10 •flush: OFF •flush_time: 0 •ft_boolean_syntax: + -><()~*:"'& •ft_max_word_len: 84 •ft_min_word_len: 4 •ft_query_expansion_limit: 20 •ft_stopword_file: (built-in) •group_concat_max_len: 1024 •have_archive: YES •have_bdb: NO •have_blackhole_engine: YES •have_compress: YES •have_crypt: YES •have_csv: YES •have_dynamic_loading: YES •have_example_engine: NO

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •have_federated_engine: YES •have_geometry: YES •have_innodb: YES •have_isam: NO •have_merge_engine: YES •have_ndbcluster: DISABLED •have_openssl: YES •have_query_cache: YES •have_raid: NO •have_rtree_keys: YES •have_ssl: YES •have_symlink: YES •hostname: metasploitable •init_connect: •init_file: •init_slave: •innodb_additional_mem_pool_size: 1048576 •innodb_autoextend_increment: 8 •innodb_buffer_pool_awesome_mem_mb: 0 •innodb_buffer_pool_size: 8388608 •innodb_checksums: ON •innodb_commit_concurrency: 0 •innodb_concurrency_tickets: 500 •innodb_data_file_path: ibdata1:10M:autoextend •innodb_data_home_dir: •innodb_doublewrite: ON •innodb_fast_shutdown: 1 •innodb_file_io_threads: 4 •innodb_file_per_table: OFF •innodb_flush_log_at_trx_commit: 1 •innodb_flush_method: •innodb_force_recovery: 0 •innodb_lock_wait_timeout: 50 •innodb_locks_unsafe_for_binlog: OFF •innodb_log_arch_dir: •innodb_log_archive: OFF •innodb_log_buffer_size: 1048576 •innodb_log_file_size: 5242880

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •innodb_log_files_in_group: 2 •innodb_log_group_home_dir: ./ •innodb_max_dirty_pages_pct: 90 •innodb_max_purge_lag: 0 •innodb_mirrored_log_groups: 1 •innodb_open_files: 300 •innodb_rollback_on_timeout: OFF •innodb_support_xa: ON •innodb_sync_spin_loops: 20 •innodb_table_locks: ON •innodb_thread_concurrency: 8 •innodb_thread_sleep_delay: 10000 •interactive_timeout: 28800 •join_buffer_size: 131072 •keep_files_on_create: OFF •key_buffer_size: 16777216 •key_cache_age_threshold: 300 •key_cache_block_size: 1024 •key_cache_division_limit: 100 •language: /usr/share/mysql/english/ •large_files_support: ON •large_page_size: 0 •large_pages: OFF •lc_time_names: en_US •license: GPL •local_infile: ON •locked_in_memory: OFF •log: OFF •log_bin: OFF •log_bin_trust_function_creators: OFF •log_error: •log_queries_not_using_indexes: OFF •log_slave_updates: OFF •log_slow_queries: OFF •log_warnings: 1 •logging: disabled •long_query_time: 10 •low_priority_updates: OFF •lower_case_file_system: OFF •lower_case_table_names: 0

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •max_allowed_packet: 16776192 •max_binlog_cache_size: 4294967295 •max_binlog_size: 104857600 •max_connect_errors: 10 •max_connections: 100 •max_delayed_threads: 20 •max_error_count: 64 •max_heap_table_size: 16777216 •max_insert_delayed_threads: 20 •max_join_size: 18446744073709551615 •max_length_for_sort_data: 1024 •max_prepared_stmt_count: 16382 •max_relay_log_size: 0 •max_seeks_for_key: 4294967295 •max_sort_length: 1024 •max_sp_recursion_depth: 0 •max_tmp_tables: 32 •max_user_connections: 0 •max_write_lock_count: 4294967295 •multi_range_count: 256 •myisam_data_pointer_size: 6 •myisam_max_sort_file_size: 2147483647 •myisam_recover_options: OFF •myisam_repair_threads: 1 •myisam_sort_buffer_size: 8388608 •myisam_stats_method: nulls_unequal •ndb_autoincrement_prefetch_sz: 32 •ndb_cache_check_time: 0 •ndb_connectstring: •ndb_force_send: ON •ndb_use_exact_count: ON •ndb_use_transactions: ON •net_buffer_length: 16384 •net_read_timeout: 30 •net_retry_count: 10 •net_write_timeout: 60 •new: OFF •old_passwords: OFF

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •open_files_limit: 1024 •optimizer_prune_level: 1 •optimizer_search_depth: 62 •pid_file: /var/run/mysqld/mysqld.pid •port: 3306 •preload_buffer_size: 32768 •profiling: OFF •profiling_history_size: 15 •protocolVersion: 10 •protocol_version: 10 •query_alloc_block_size: 8192 •query_cache_limit: 1048576 •query_cache_min_res_unit: 4096 •query_cache_size: 16777216 •query_cache_type: ON •query_cache_wlock_invalidate: OFF •query_prealloc_size: 8192 •range_alloc_block_size: 2048 •read_buffer_size: 131072 •read_only: OFF •read_rnd_buffer_size: 262144 •relay_log_purge: ON •relay_log_space_limit: 0 •rpl_recovery_rank: 0 •secure_auth: OFF •secure_file_priv: •server_id: 0 •skip_external_locking: ON •skip_networking: OFF •skip_show_database: OFF •slave_compressed_protocol: OFF •slave_load_tmpdir: /tmp/ •slave_net_timeout: 3600 •slave_skip_errors: OFF •slave_transaction_retries: 10 •slow_launch_time: 2 •socket: /var/run/mysqld/mysqld.sock •sort_buffer_size: 2097144 •sql_big_selects: ON •sql_mode: STRICT_TRANS_TABLES

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •sql_notes: ON •sql_warnings: OFF •ssl_ca: /etc/mysql/cacert.pem •ssl_capath: •ssl_cert: /etc/mysql/server-cert.pem •ssl_cipher: •ssl_key: /etc/mysql/server-key.pem •storage_engine: MyISAM •sync_binlog: 0 •sync_frm: ON •system_time_zone: EDT •table_cache: 64 •table_lock_wait_timeout: 50 •table_type: MyISAM •thread_cache_size: 8 •thread_stack: 131072 •time_format: %H:%i:%s •time_zone: SYSTEM •timed_mutexes: OFF •tmp_table_size: 33554432 •tmpdir: /tmp •transaction_alloc_block_size: 8192 •transaction_prealloc_size: 4096 •tx_isolation: REPEATABLE-READ •updatable_views_with_limit: YES •version: 5.0.51a-3ubuntu5 •version_comment: (Ubuntu) •version_compile_machine: i486 •version_compile_os: debian-linux-gnu •wait_timeout: 28800

4.9. NFS

4.9.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	udp	2049	0	<ul style="list-style-type: none"> •program-number: 100003 •program-version: 4
192.168.0.102	tcp	2049	0	<ul style="list-style-type: none"> •program-number: 100003 •program-version: 4

4.10. NFS lockd

4.10.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	37506	0	<ul style="list-style-type: none"> •program-number: 100021 •program-version: 4
192.168.0.102	udp	56422	0	<ul style="list-style-type: none"> •program-number: 100021 •program-version: 4

4.11. Postgres

4.11.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	5432	0	

4.12. Remote Execution

4.12.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	512	1	

4.13. Remote Login

4.13.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	513	1	

4.14. Remote Shell

4.14.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	514	1	

4.15. SMTP

4.15.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
--------	----------	------	-----------------	------------------------

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	25	1	<ul style="list-style-type: none"> •Postfix 2.5.1 •advertised-esmtp-extension-count: 8 •advertises-esmtp: TRUE •max-message-size: 10240000 •smtp.plaintext.authentication: false •supports-8bitmime: TRUE •supports-debug: FALSE •supports-dsn: TRUE •supports-enhancedstatuscodes: TRUE •supports-etn: TRUE •supports-expand: FALSE •supports-pipelining: TRUE •supports-size: TRUE •supports-starttls: TRUE •supports-turn: FALSE •supports-verify: FALSE •supports-vrfy: TRUE

4.16. SSH

4.16.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	22	2	<ul style="list-style-type: none"> •OpenBSD OpenSSH 4.7p1 •ssh.banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 •ssh.protocol.version: 2.0 •ssh.rsa.pubkey.fingerprint: 5656240F211DDEA72BAE61B1243DE8F3

4.17. Shell Backdoor

4.17.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	1524	1	<ul style="list-style-type: none"> •system: unix •unix.shell: bash

4.18. Telnet

4.18.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	23	1	

4.19. VNC

4.19.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	5900	2	<ul style="list-style-type: none"> •protocol-version: 3.3 •supported-auth-1: VNC Authentication •supported-auth-count: 1

4.20. XWindows

4.20.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	6000	0	

4.21. ajp13 (Apache JServ Protocol 1.3)

4.21.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	8009	0	

4.22. irc (Internet Relay Chat)

4.22.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	tcp	6667	0	

4.23. mountd

4.23.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	udp	34478	1	<ul style="list-style-type: none"> •program-number: 100005 •program-version: 3
192.168.0.102	tcp	39883	1	

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none">•program-number: 100005•program-version: 3

4.24. portmapper

4.24.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	udp	111	0	<ul style="list-style-type: none">•program-number: 100000•program-version: 2
192.168.0.102	tcp	111	0	<ul style="list-style-type: none">•program-number: 100000•program-version: 2

4.25. status

4.25.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.102	udp	40809	0	<ul style="list-style-type: none">•program-number: 100024•program-version: 1
192.168.0.102	tcp	58715	0	<ul style="list-style-type: none">•program-number: 100024•program-version: 1

5. Discovered Users and Groups

5.1. System

5.1.1. 192.168.0.102

Account Name	Type	Additional Information
AnonymousLogon	Group	<ul style="list-style-type: none"> •comment: AnonymousLogon •group-id: 7
Authenticated Users	Group	<ul style="list-style-type: none"> •comment: Authenticated Users •group-id: 11
Batch	Group	<ul style="list-style-type: none"> •comment: Batch •group-id: 3
Creator Group	Group	<ul style="list-style-type: none"> •comment: Creator Group •group-id: 1
Creator Owner	Group	<ul style="list-style-type: none"> •comment: Creator Owner
Dialup	Group	<ul style="list-style-type: none"> •comment: Dialup •group-id: 1
Everyone	Group	<ul style="list-style-type: none"> •comment: Everyone
Interactive	Group	<ul style="list-style-type: none"> •comment: Interactive •group-id: 4
Local Service	Group	<ul style="list-style-type: none"> •comment: Local Service •group-id: 19
Network	Group	<ul style="list-style-type: none"> •comment: Network •group-id: 2
Network Service	Group	<ul style="list-style-type: none"> •comment: Network Service •group-id: 20
Proxy	Group	<ul style="list-style-type: none"> •comment: Proxy •group-id: 8
Remote Interactive Logon	Group	<ul style="list-style-type: none"> •comment: Remote Interactive Logon •group-id: 14
Restricted	Group	<ul style="list-style-type: none"> •comment: Restricted •group-id: 12
SYSTEM	Group	<ul style="list-style-type: none"> •comment: SYSTEM

Account Name	Type	Additional Information
		•group-id: 18
Self	Group	•comment: Self •group-id: 10
ServerLogon	Group	•comment: ServerLogon •group-id: 9
Service	Group	•comment: Service •group-id: 6
Terminal Server User	Group	•comment: Terminal Server User •group-id: 13
This Organization	Group	•comment: This Organization •group-id: 15
adm	Group	•group-id: 4
admin	Group	•group-id: 112
audio	Group	•group-id: 29
backup	Group	•group-id: 34
bin	User	•gid: 2 •loginShell: /bin/sh •password: x •user-id: 2 •userDir: /bin
bind	User	•gid: 113 •loginShell: /bin/false •password: x •user-id: 105 •userDir: /var/cache/bind
cdrom	Group	•group-id: 24
crontab	Group	•group-id: 108
daemon	User	•comment: •user-id: 1002
dhcp	User	•gid: 102 •loginShell: /bin/false •password: x •user-id: 101 •userDir: /nonexistent

Account Name	Type	Additional Information
dialout	Group	•group-id: 20
dip	Group	•group-id: 30
disk	Group	•group-id: 6
distccd	User	•gid: 65534 •loginShell: /bin/false •password: x •user-id: 111 •userDir: /
fax	Group	•group-id: 21
floppy	Group	•group-id: 25
ftp	User	•comment: •user-id: 1214
fuse	Group	•group-id: 107
games	User	•comment: •user-id: 1010
gnats	User	•comment: •full-name: Gnats Bug-Reporting System (admin) •user-id: 1082
irc	Group	•group-id: 39
klog	Group	•group-id: 104
kmem	Group	•group-id: 15
libuuid	User	•gid: 101 •loginShell: /bin/sh •password: x •user-id: 100 •userDir: /var/lib/libuuid
list	User	•full-name: Mailing List Manager •gid: 38 •loginShell: /bin/sh •password: x •user-id: 38 •userDir: /var/list
lp	Group	•group-id: 7
lpadmin	Group	•group-id: 111

Account Name	Type	Additional Information
mail	User	<ul style="list-style-type: none"> •gid: 8 •loginShell: /bin/sh •password: x •user-id: 8 •userDir: /var/mail
man	Group	<ul style="list-style-type: none"> •group-id: 12
mlocate	Group	<ul style="list-style-type: none"> •group-id: 109
msfadmin	User	<ul style="list-style-type: none"> •comment: •full-name: msfadmin,,, •user-id: 3000
mysql	User	<ul style="list-style-type: none"> •full-name: MySQL Server,,, •gid: 118 •loginShell: /bin/false •password: x •user-id: 109 •userDir: /var/lib/mysql
news	User	<ul style="list-style-type: none"> •comment: •user-id: 1018
nobody	User	<ul style="list-style-type: none"> •gid: 65534 •loginShell: /bin/sh •password: x •user-id: 65534 •userDir: /nonexistent
nogroup	Group	<ul style="list-style-type: none"> •group-id: 65534
nvram	Group	<ul style="list-style-type: none"> •group-id: 106
operator	Group	<ul style="list-style-type: none"> •group-id: 37
plugdev	Group	<ul style="list-style-type: none"> •group-id: 46
postdrop	Group	<ul style="list-style-type: none"> •group-id: 116
postfix	User	<ul style="list-style-type: none"> •comment: •user-id: 1212
postgres	User	<ul style="list-style-type: none"> •full-name: PostgreSQL administrator,,, •gid: 117 •loginShell: /bin/bash •password: x •user-id: 108

Account Name	Type	Additional Information
		•userDir: /var/lib/postgresql
proftpd	User	•comment: •user-id: 1226
proxy	User	•comment: •user-id: 1026
root	User	•gid: 0 •loginShell: /bin/bash •password: x •userDir: /root
sambashare	Group	•group-id: 119
sasl	Group	•group-id: 45
scanner	Group	•group-id: 105
service	User	•full-name: ,,, •gid: 1002 •loginShell: /bin/bash •password: x •user-id: 1002 •userDir: /home/service
shadow	Group	•group-id: 42
snmp	User	•gid: 65534 •loginShell: /bin/false •password: x •user-id: 115 •userDir: /var/lib/snmp
src	Group	•group-id: 40
ssh	Group	•group-id: 110
sshd	User	•gid: 65534 •loginShell: /usr/sbin/nologin •password: x •user-id: 104 •userDir: /var/run/sshd
ssl-cert	Group	•group-id: 114
staff	Group	•group-id: 50
statd	User	•gid: 65534

Account Name	Type	Additional Information
		<ul style="list-style-type: none"> •loginShell: /bin/false •password: x •user-id: 114 •userDir: /var/lib/nfs
sudo	Group	•group-id: 27
sync	User	<ul style="list-style-type: none"> •comment: •user-id: 1008
sys	Group	•group-id: 3
syslog	User	<ul style="list-style-type: none"> •comment: •user-id: 1204
tape	Group	•group-id: 26
telnetd	Group	•group-id: 120
tomcat55	User	<ul style="list-style-type: none"> •gid: 65534 •loginShell: /bin/false •password: x •user-id: 110 •userDir: /usr/share/tomcat5.5
tty	Group	•group-id: 5
user	User	<ul style="list-style-type: none"> •comment: •full-name: just a user,111,, •user-id: 3002
users	Group	•group-id: 100
utmp	Group	•group-id: 43
uucp	Group	•group-id: 10
video	Group	•group-id: 44
voice	Group	•group-id: 22
www-data	Group	•group-id: 33

5.2. MySQL

5.2.1. 192.168.0.102

Account Name	Type	Additional Information
debian-sys-maint	User	

Audit Report

Account Name	Type	Additional Information
guest	User	
root	User	

6. Discovered Databases

6.1. MySQL

6.1.1. 192.168.0.102

- dvwa
- information_schema
- metasploit
- mysql
- owasp10
- tikiwiki
- tikiwiki195

7. Discovered Files and Directories

7.1. 192.168.0.102

File/Directory Name	Type	Properties
opt	Directory	<ul style="list-style-type: none">•comment:•mount-point: C:\tmp
print\$	Directory	<ul style="list-style-type: none">•comment: Printer Drivers•mount-point: C:\var\lib\samba\printers
tmp	Directory	<ul style="list-style-type: none">•comment: oh noes!•mount-point: C:\tmp

8. Policy Evaluations

No policy evaluations were performed.

9. Spidered Web Sites

No web sites were spidered during the scan.