Audit Report

meta full nexpose scan

Audited on November 30, 2019

Reported on November 30, 2019

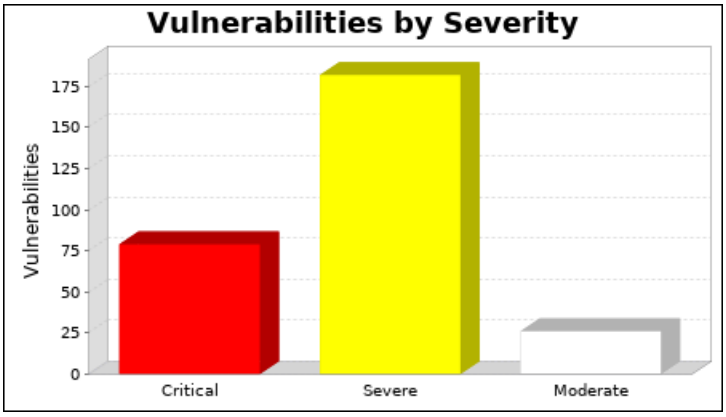
1. Executive Summary

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.

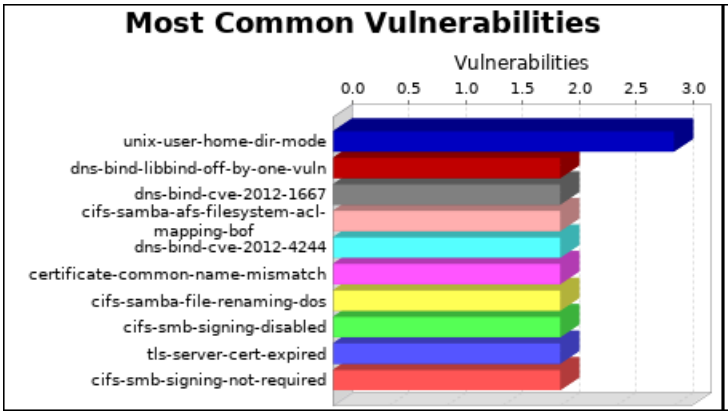
Site Name	Start Time	End Time	Total Time	Status
meta full	November 30, 2019 06:16, PST	November 30, 2019 06:21, PST	5 minutes	Success

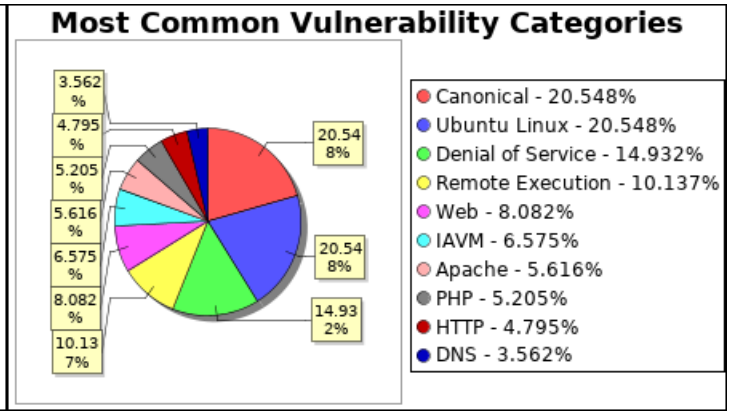
There is not enough historical data to display risk trend.

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

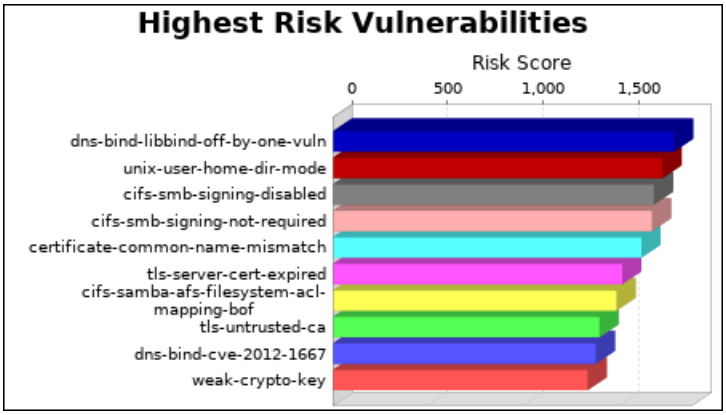


There were 287 vulnerabilities found during this scan. Of these, 79 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 182 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 26 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.

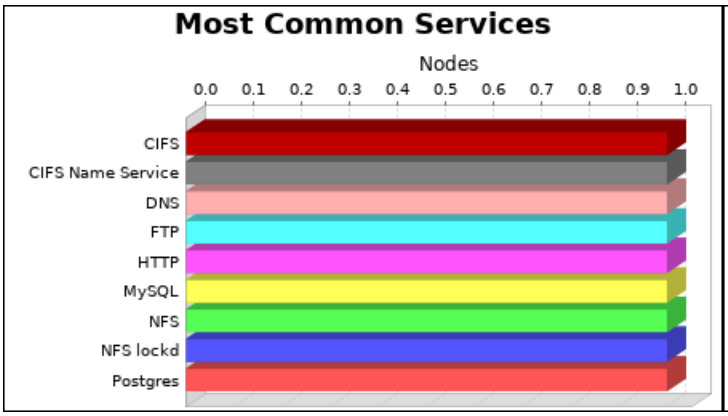


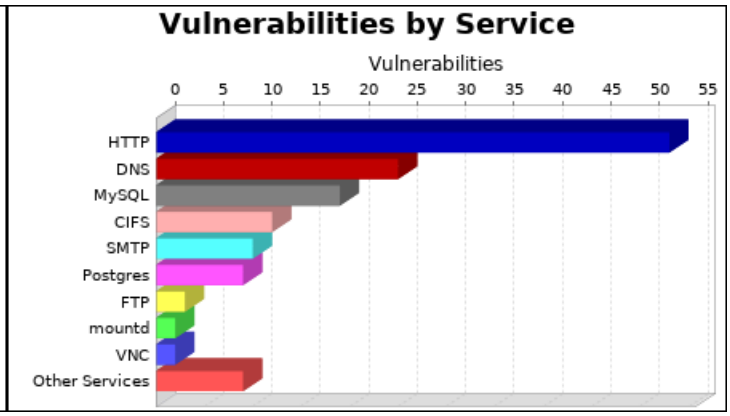


There were 3 occurrences of the unix-user-home-dir-mode vulnerability, making it the most common vulnerability. There were 150 vulnerability instances in the Canonical and Ubuntu Linux categories, making them the most common vulnerability categories.



The dns-bind-libbind-off-by-one-vuln vulnerability poses the highest risk to the organization with a risk score of 1,781. Risk scores are based on the types and numbers of vulnerabilities on affected assets.
One operating system was identified during this scan.
There were 21 services found to be running during this scan.





The CIFS, CIFS Name Service, DNS, FTP, HTTP, MySQL, NFS, NFS lockd and Postgres 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 53 vulnerabilities.

2. Discovered Systems

Node	Operating System	Risk	Aliases
10.0.2.4	Ubuntu Linux 8.04	158,551	•METASPLOITABLE •metasploitable •metasploitable.localdomain

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

3.1.1. Default Tomcat User and Password (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:
10.0.2.4:8180	Running HTTP serviceProduct Tomcat exists -- Apache TomcatBased on the following 2 results:HTTP GET request to http://10.0.2.4:8180/manager/html HTTP response code was an expected 401 HTTP GET request to http://10.0.2.4:8180/manager/html HTTP response code was an expected 200 78: <img border="0" alt="The Apache Software Foundation" align="left" 79: src="/manager/images/asf-logo.gif"> 80: 81: <a href="http://tomcat.apache.org/"> 82: ...="0" alt="The Tomcat Servlet/JSP Container"

References:

Source	Reference
BID	38084
CVE	CVE-2009-3843
CVE	CVE-2010-0557
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: Buffer overflow in inet_network() (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:
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 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	10190
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:
10.0.2.4	Execute command: env x='() { :;}; echo CVE-2014-6271' bash -c exit 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:
10.0.2.4	Execute command: x='() { echo Vulnerable; }' bash -c x 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:
10.0.2.4	Execute command: mkdir -m 0700 ~/.rapid7_tmp; cd ~/.rapid7_tmp && (rm -f shellShockOutput; echo "env X='() { (a)=>\' bash -c 'shellShockOutput echo CVE-2014-7169"' | bash; cat shellShockOutput; rm shellShockOutput) Standard output matched: 1: bash: X: line 1: syntax error near unexpected token `=' 2: bash: X: line 1: `' 3: bash: error importing function definition for `X' 4: CVE-2014-7169

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:
10.0.2.4	Execute command: bash -c "echo 'Check that bash is available"' && (bash -c 'true <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF' || echo CVE-2014-7186) Standard output matched: 1: Check that bash is available

Affected Nodes:	Additional Information:
	2: 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. CVE-2014-7187 bash: off-by-one error in deeply nested flow control constructs (gnu-bash-cve-2014-7187)

Description:

Off-by-one error in the read_token_word function 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 deeply nested for loops, aka the "word_lineno" issue.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4	Execute command: bash -c "echo 'Check that bash is available'" && bash -c '[["1 2 3 4 5" == `echo {1..5}`]]' && (bash -c '(for i in {1..200}; do echo "for x$i in; do :;"; done; for i in {1..200}; do echo "done;";done)' | bash || echo "CVE-2014-7187") Standard output matched: 1: Check that bash is available 2: bash: line 129: syntax error near `x129' 3: bash: line 129: `for x129 in; do :;' 4: CVE-2014-7187

References:

Source	Reference
CVE	CVE-2014-7187

Vulnerability Solution:

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

3.1.8. 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:
10.0.2.4:3306	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

3.1.9. 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:
10.0.2.4:80	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
BID	54638
CVE	CVE-2012-2688
DEBIAN	DSA-2527
REDHAT	RHSA-2013:1307
XF	77155

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/

3.1.10. 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:
10.0.2.4:1524	Running Shell Backdoor service

References:

None

Vulnerability Solution:

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

3.1.11. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04

References:

None

Vulnerability Solution:

Upgrade to a supported version of Ubuntu Linux

3.1.12. 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:
10.0.2.4	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
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

Source	Reference
USN	1403-1

Vulnerability Solution:

libfreetype6 on Ubuntu Linux

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

3.1.13. 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:
10.0.2.4	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	1423-1

Vulnerability Solution:

samba on Ubuntu Linux

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

3.1.14. USN-613-1: GnuTLS vulnerabilities (ubuntu-usn-613-1)

Description:

The _gnutls_server_name_recv_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:
10.0.2.4	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	10935
OVAL	11393
OVAL	9519
REDHAT	RHSA-2008:0489
REDHAT	RHSA-2008:0492
SUSE	SUSE-SA:2008:046
USN	613-1
XF	42530
XF	42532
XF	42533

Vulnerability Solution:

libgnutls13 on Ubuntu Linux

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

3.1.15. 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:
10.0.2.4	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	11760
OVAL	6103
OVAL	6496
OVAL	9812
REDHAT	RHSA-2008:0836
REDHAT	RHSA-2008:0884
REDHAT	RHSA-2008:0886
USN	644-1
XF	45085

Vulnerability Solution:

libxml2 on Ubuntu Linux

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

3.1.16. 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:
10.0.2.4	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	10025
OVAL	6219
OVAL	6234
OVAL	6360
OVAL	6415
OVAL	9888
REDHAT	RHSA-2008:0988
USN	673-1

Vulnerability Solution:

libxml2 on Ubuntu Linux

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

3.1.17. 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:
10.0.2.4	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	762-1

Vulnerability Solution:

apt on Ubuntu Linux

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

3.1.18. 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:
10.0.2.4	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

Source	Reference
OVAL	10758
OVAL	5941
REDHAT	RHSA-2009:1136
REDHAT	RHSA-2009:1154
SUSE	SUSE-SA:2009:037
USN	803-1

Vulnerability Solution:

•dhcp3-client on Ubuntu Linux

Upgrade dhcp3-client

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

•dhcp3-client-udeb on Ubuntu Linux

Upgrade dhcp3-client-udeb

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

3.1.19. 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:
10.0.2.4	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

Source	Reference
OVAL	8394
OVAL	9958
SUSE	SUSE-SA:2009:050
USN	813-1

Vulnerability Solution:

libapr1 on Ubuntu Linux

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

3.1.20. 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:
10.0.2.4	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	8394
OVAL	9958
SUSE	SUSE-SA:2009:050
USN	813-3

Vulnerability Solution:

libaprutil1 on Ubuntu Linux
Use `apt-get upgrade` to upgrade libaprutil1 to the latest version.

3.1.21. 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:
10.0.2.4	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
OVAL	10129
OVAL	11760
OVAL	6103
OVAL	7783

Source	Reference
OVAL	8639
OVAL	9262
REDHAT	RHSA-2008:0884
REDHAT	RHSA-2008:0886
USN	815-1
XF	45085

Vulnerability Solution:

libxml2 on Ubuntu Linux

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

3.1.22. 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:
10.0.2.4:5900	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.

3.1.23. 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:

Affected Nodes:	Additional Information:
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 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	53772
CERT-VN	381699
CVE	CVE-2012-1667
DEBIAN	DSA-2486
DISA_SEVERITY	Category I
DISA_VMSKEY	V0035032
IAVM	2012-A-0189
REDHAT	RHSA-2012:0717
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.

3.1.24. 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:
10.0.2.4:80	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

3.1.25. '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:
10.0.2.4:512	Running Remote Execution service

References:

None

Vulnerability Solution:

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

3.1.26. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04

Affected Nodes:	Additional Information:
	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
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	1013-1

Vulnerability Solution:

libfreetype6 on Ubuntu Linux

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

3.1.27. 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:
10.0.2.4	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	1085-1

Vulnerability Solution:

libtiff4 on Ubuntu Linux

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

3.1.28. 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:
10.0.2.4	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
IAVM	2012-A-0073
IAVM	2012-A-0153
OSVDB	73248
REDHAT	RHSA-2011:1749
REDHAT	RHSA-2013:0217
USN	1153-1

Vulnerability Solution:

libxml2 on Ubuntu Linux

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

3.1.29. 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:
10.0.2.4	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
APPLE	APPLE-SA-2012-02-01-1
BID	50155
CVE	CVE-2011-3256
CVE	CVE-2011-3439
DEBIAN	DSA-2328
USN	1267-1
XF	70552

Vulnerability Solution:

libfreetype6 on Ubuntu Linux

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

3.1.30. 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:
10.0.2.4	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	13840
OVAL	14410
OVAL	14504
OVAL	14761
REDHAT	RHSA-2011:1749
REDHAT	RHSA-2013:0217
USN	1334-1
XF	69885

Vulnerability Solution:

libxml2 on Ubuntu Linux

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

3.1.31. 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:
10.0.2.4	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
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

Source	Reference
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	1357-1
XF	72129

Vulnerability Solution:

•libssl0.9.8 on Ubuntu Linux

Upgrade libssl0.9.8

Use `apt-get upgrade` to upgrade libssl0.9.8 to the latest version.

•libssl1.0.0 on Ubuntu Linux

Upgrade libssl1.0.0

Use `apt-get upgrade` to upgrade libssl1.0.0 to the latest version.

•openssl on Ubuntu Linux

Upgrade openssl

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

3.1.32. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu mysql-server-5.0 5.0.51a-3ubuntu5

References:

Source	Reference

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
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

Source	Reference
CVE	CVE-2008-3963
CVE	CVE-2008-4098
CVE	CVE-2008-4456
CVE	CVE-2008-7247
CVE	CVE-2009-2446
CVE	CVE-2009-4019
CVE	CVE-2009-4030
CVE	CVE-2009-4484
CVE	CVE-2010-1621
CVE	CVE-2010-1626
CVE	CVE-2010-1848
CVE	CVE-2010-1849
CVE	CVE-2010-1850
CVE	CVE-2010-2008
CVE	CVE-2010-3677
CVE	CVE-2010-3678
CVE	CVE-2010-3679
CVE	CVE-2010-3680
CVE	CVE-2010-3681
CVE	CVE-2010-3682
CVE	CVE-2010-3683
CVE	CVE-2010-3833
CVE	CVE-2010-3834
CVE	CVE-2010-3835
CVE	CVE-2010-3836
CVE	CVE-2010-3837
CVE	CVE-2010-3838
CVE	CVE-2010-3839
CVE	CVE-2010-3840
CVE	CVE-2011-2262
CVE	CVE-2012-0075
CVE	CVE-2012-0087
CVE	CVE-2012-0101

Source	Reference
CVE	CVE-2012-0102
CVE	CVE-2012-0112
CVE	CVE-2012-0113
CVE	CVE-2012-0114
CVE	CVE-2012-0115
CVE	CVE-2012-0116
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

Source	Reference
OSVDB	78375
OSVDB	78377
OSVDB	78378
OSVDB	78379
OSVDB	78383
OSVDB	78384
OSVDB	78385
OSVDB	78386
OSVDB	78387
OSVDB	78388
OSVDB	78389
OSVDB	78390
OSVDB	78393
OSVDB	78394
OVAL	10258
OVAL	10521
OVAL	10591
OVAL	10846
OVAL	11116
OVAL	11349
OVAL	11390
OVAL	11456
OVAL	11857
OVAL	11869
OVAL	6693
OVAL	7210
OVAL	7328
OVAL	8156
OVAL	8500
OVAL	9490
REDHAT	RHSA-2007:1155
REDHAT	RHSA-2007:1157
REDHAT	RHSA-2009:1067

Source	Reference
REDHAT	RHSA-2009:1289
REDHAT	RHSA-2010:0109
REDHAT	RHSA-2010:0110
REDHAT	RHSA-2010:0442
REDHAT	RHSA-2010:0824
REDHAT	RHSA-2010:0825
REDHAT	RHSA-2011:0164
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

Source	Reference
XF	72526
XF	72527
XF	72528
XF	72529
XF	72530
XF	72531
XF	72532
XF	72533
XF	72537
XF	72538
XF	72539
XF	72540

Vulnerability Solution:

•mysql-server-5.0 on Ubuntu Linux

Upgrade mysql-server-5.0

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

•mysql-server-5.1 on Ubuntu Linux

Upgrade mysql-server-5.1

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

3.1.33. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu postgresql-8.3 8.3.1-1

References:

Source	Reference

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	1789-1

Vulnerability Solution:

•postgresql-8.3 on Ubuntu Linux

Upgrade postgresql-8.3

Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version.

•postgresql-8.4 on Ubuntu Linux

Upgrade postgresql-8.4

Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version.

•postgresql-9.1 on Ubuntu Linux

Upgrade postgresql-9.1

Use `apt-get upgrade` to upgrade postgresql-9.1 to the latest version.

3.1.34. 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:
10.0.2.4	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

Source	Reference
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	10020
OVAL	11132
OVAL	5643
OVAL	5733
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	617-1
XF	38501
XF	42664
XF	45251

Vulnerability Solution:

•libsmbclient on Ubuntu Linux

Upgrade libsmbclient

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

•samba on Ubuntu Linux

Upgrade samba

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

3.1.35. 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:
10.0.2.4	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
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	10434
OVAL	10790
OVAL	7087
OVAL	7090
OVAL	7211
OVAL	7257

Source	Reference
OVAL	7292
OVAL	7791
OVAL	9191
OVAL	9944
USN	839-1
XF	51327
XF	51328
XF	53174
XF	53574
XF	53575

Vulnerability Solution:

•samba on Ubuntu Linux

Upgrade samba

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

•smbclient on Ubuntu Linux

Upgrade smbclient

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

•smbfs on Ubuntu Linux

Upgrade smbfs

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

3.1.36. 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:
10.0.2.4	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
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	10591
OVAL	11116
OVAL	11349
OVAL	11456
OVAL	11857
OVAL	8156
OVAL	8500
REDHAT	RHSA-2009:1067
REDHAT	RHSA-2009:1289
REDHAT	RHSA-2010:0109
REDHAT	RHSA-2010:0110
USN	897-1
XF	45590

Source	Reference
XF	45649
XF	51614
XF	55416

Vulnerability Solution:

•mysql-server-5.0 on Ubuntu Linux

Upgrade mysql-server-5.0

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

•mysql-server-5.1 on Ubuntu Linux

Upgrade mysql-server-5.1

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

3.1.37. 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:
10.0.2.4	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

Source	Reference
CVE	CVE-2010-2805
CVE	CVE-2010-2806
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	972-1
XF	60856

Vulnerability Solution:

libfreetype6 on Ubuntu Linux

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

3.1.38. Apache HTTPD: Range header remote DoS (CVE-2011-3192) (apache-httpd-cve-2011-3192)

Description:

A flaw was found in the way the Apache HTTP Server handled Range HTTP headers. A remote attacker could use this flaw to cause httpd to use an excessive amount of memory and CPU time via HTTP requests with a specially-crafted Range header. This could be used in a denial of service attack. Advisory: CVE-2011-3192.txt

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	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-2011-10-12-3
BID	49303
CERT-VN	405811
CVE	CVE-2011-3192
OVAL	14762

Source	Reference
OVAL	14824
OVAL	18827
REDHAT	RHSA-2011:1245
REDHAT	RHSA-2011:1294
REDHAT	RHSA-2011:1300
REDHAT	RHSA-2011:1329
REDHAT	RHSA-2011:1330
REDHAT	RHSA-2011:1369
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	69396

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 < 2.2.20

Upgrade to Apache HTTPD version 2.2.20

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.20.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.

3.1.39. Apache HTTPD: ap_get_basic_auth_pw() Authentication Bypass (CVE-2017-3167) (apache-httpd-cve-2017-3167)

Description:

Use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed. Third-party module writers SHOULD use ap_get_basic_auth_components(), available in 2.2.34 and 2.4.26, instead of ap_get_basic_auth_pw(). Modules which call the legacy ap_get_basic_auth_pw() during the authentication phase MUST either immediately authenticate the user after the call, or else stop the request immediately with an error response, to avoid incorrectly authenticating the current request.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
BID	99135
CVE	CVE-2017-3167
DEBIAN	DSA-3896
REDHAT	RHSA-2017:2478
REDHAT	RHSA-2017:2479
REDHAT	RHSA-2017:2483
REDHAT	RHSA-2017:3193
REDHAT	RHSA-2017:3194
REDHAT	RHSA-2017:3195
REDHAT	RHSA-2017:3475
REDHAT	RHSA-2017:3476
REDHAT	RHSA-2017:3477
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 < 2.2.34

Upgrade to Apache HTTPD version 2.2.34

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.34.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 < 2.4.26

Upgrade to Apache HTTPD version 2.4.26

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.26.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.

3.1.40. Apache HTTPD: mod_ssl Null Pointer Dereference (CVE-2017-3169) (apache-httpd-cve-2017-3169)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_ssl. Review your web server configuration for validation. mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
BID	99134
CVE	CVE-2017-3169
DEBIAN	DSA-3896
REDHAT	RHSA-2017:2478
REDHAT	RHSA-2017:2479
REDHAT	RHSA-2017:2483
REDHAT	RHSA-2017:3193
REDHAT	RHSA-2017:3194
REDHAT	RHSA-2017:3195
REDHAT	RHSA-2017:3475
REDHAT	RHSA-2017:3476
REDHAT	RHSA-2017:3477
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 < 2.2.34

Upgrade to Apache HTTPD version 2.2.34

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.34.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 < 2.4.26

Upgrade to Apache HTTPD version 2.4.26

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.26.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.

3.1.41. Apache HTTPD: mod_mime Buffer Overread (CVE-2017-7679) (apache-httpd-cve-2017-7679)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_mime. Review your web server configuration for validation. mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
BID	99170
CVE	CVE-2017-7679
DEBIAN	DSA-3896
REDHAT	RHSA-2017:2478
REDHAT	RHSA-2017:2479
REDHAT	RHSA-2017:2483
REDHAT	RHSA-2017:3193
REDHAT	RHSA-2017:3194
REDHAT	RHSA-2017:3195
REDHAT	RHSA-2017:3475
REDHAT	RHSA-2017:3476
REDHAT	RHSA-2017:3477
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 < 2.2.34

Upgrade to Apache HTTPD version 2.2.34

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.34.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 < 2.4.26

Upgrade to Apache HTTPD version 2.4.26

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.26.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.

3.1.42. 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:
10.0.2.4:8180	Running HTTP serviceProduct Tomcat exists -- Apache TomcatHTTP GET request to http://10.0.2.4:8180/tomcat-docs/appdev/sample/web/hello.jsp HTTP response code was an expected 200 15: limitations under the License. 16: --> 17: <html> 18: <head> 19: <title>Sample Application JSP Page</title>

References:
None

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

3.1.43. 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:
10.0.2.4:5900	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 provides additional information on available strong password mechanisms when authenticating.
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 or General Docs or FAQ.

3.1.44. 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:
10.0.2.4	Found user(s) via named pipes.Found server name via named pipes.Found local group(s) via named pipes.

References:

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

Vulnerability Solution:

•Microsoft Windows Server 2016, Microsoft Windows Server 2016 Standard Edition, Microsoft Windows Server 2016 Essentials Edition, Microsoft Windows Server 2016 Datacenter Edition, Microsoft Windows Storage Server 2016

Disable NULL sessions for Windows 2016

Open Local Security Settings, and disable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Allow anonymous SID/Name translation: Disabled,
Network access: Let Everyone permissions apply to anonymous users : Disabled

Open Local Security Settings, and enable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Do not allow anonymous enumeration of SAM accounts: Enabled,
Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled,
Network access: Restrict anonymous access to Named Pipes and Shares: Enabled

Open Local Security Settings, and apply an empty list to the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Named Pipes that can be accessed anonymously,
Network access: Shares that can be accessed anonymously

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 10, Microsoft Windows 10 Education Edition, Microsoft Windows 10 Enterprise Edition, Microsoft Windows 10 Home Edition, Microsoft Windows 10 Mobile Enterprise Edition, Microsoft Windows 10 Mobile Edition, Microsoft Windows 10 Professional Edition
Disable NULL sessions for Windows 10
Open Local Security Settings from Administrative Tools, and disable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Allow anonymous SID/Name translation: Disabled,
Network access: Let Everyone permissions apply to anonymous users : Disabled

Open Local Security Settings, and enable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Do not allow anonymous enumeration of SAM accounts: Enabled,
Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled,
Network access: Restrict anonymous access to Named Pipes and Shares: Enabled

Open Local Security Settings, and apply an empty list to the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Named Pipes that can be accessed anonymously,
Network access: Shares that can be accessed anonymously

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 Server 2012 R2, Microsoft Windows Server 2012 R2 Standard Edition, Microsoft Windows Server 2012 R2 Essentials Edition, Microsoft Windows Server 2012 R2 Datacenter Edition, Microsoft Windows Server 2012 R2 Foundation Edition, Microsoft Windows Storage Server 2012 R2
Disable NULL sessions for Windows 2012 R2
Open Local Security Settings, and disable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Allow anonymous SID/Name translation: Disabled,
Network access: Let Everyone permissions apply to anonymous users : Disabled

Open Local Security Settings, and enable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Do not allow anonymous enumeration of SAM accounts: Enabled,
Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled,
Network access: Restrict anonymous access to Named Pipes and Shares: Enabled

Open Local Security Settings, and apply an empty list to the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Named Pipes that can be accessed anonymously,
Network access: Shares that can be accessed anonymously

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 8.1, Microsoft Windows 8.1 Enterprise Edition, Microsoft Windows 8.1 Professional Edition
Disable NULL sessions for Windows 8.1
Open Local Security Settings from Administrative Tools, and disable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Allow anonymous SID/Name translation: Disabled,
Network access: Let Everyone permissions apply to anonymous users : Disabled

Open Local Security Settings, and enable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Do not allow anonymous enumeration of SAM accounts: Enabled,
Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled,
Network access: Restrict anonymous access to Named Pipes and Shares: Enabled

Open Local Security Settings, and apply an empty list to the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Named Pipes that can be accessed anonymously,
Network access: Shares that can be accessed anonymously

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 Server 2012, Microsoft Windows Server 2012 Standard Edition, Microsoft Windows Server 2012 Essentials Edition, Microsoft Windows Server 2012 Datacenter Edition, Microsoft Windows Server 2012 Foundation Edition, Microsoft Windows Storage Server 2012

Disable NULL sessions for Windows 2012
Open Local Security Settings, and disable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Allow anonymous SID/Name translation: Disabled,
Network access: Let Everyone permissions apply to anonymous users : Disabled

Open Local Security Settings, and enable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Do not allow anonymous enumeration of SAM accounts: Enabled,
Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled,
Network access: Restrict anonymous access to Named Pipes and Shares: Enabled

Open Local Security Settings, and apply an empty list to the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Named Pipes that can be accessed anonymously,
Network access: Shares that can be accessed anonymously

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 8, Microsoft Windows 8 Enterprise Edition, Microsoft Windows 8 Professional Edition
Disable NULL sessions for Windows 8
Open Local Security Settings from Administrative Tools, and disable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Allow anonymous SID/Name translation: Disabled,
Network access: Let Everyone permissions apply to anonymous users : Disabled

Open Local Security Settings, and enable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Do not allow anonymous enumeration of SAM accounts: Enabled,
Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled,
Network access: Restrict anonymous access to Named Pipes and Shares: Enabled

Open Local Security Settings, and apply an empty list to the following settings:

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

Network access: Named Pipes that can be accessed anonymously,
Network access: Shares that can be accessed anonymously

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 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
Disable NULL sessions for Windows 2008 R2
Open Local Security Settings, and disable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Allow anonymous SID/Name translation: Disabled,
Network access: Let Everyone permissions apply to anonymous users : Disabled

Open Local Security Settings, and enable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Do not allow anonymous enumeration of SAM accounts: Enabled,
Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled,
Network access: Restrict anonymous access to Named Pipes and Shares: Enabled

Open Local Security Settings, and apply an empty list to the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Named Pipes that can be accessed anonymously,
Network access: Shares that can be accessed anonymously

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 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
Disable NULL sessions for Windows 7
Open Local Security Settings from Administrative Tools, and disable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Allow anonymous SID/Name translation: Disabled,
Network access: Let Everyone permissions apply to anonymous users : Disabled

Open Local Security Settings, and enable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Do not allow anonymous enumeration of SAM accounts: Enabled,
Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled,
Network access: Restrict anonymous access to Named Pipes and Shares: Enabled

Open Local Security Settings, and apply an empty list to the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Named Pipes that can be accessed anonymously,
Network access: Shares that can be accessed anonymously

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 Server 2008, Microsoft Windows Server 2008 Standard Edition, Microsoft Windows Server 2008 Enterprise Edition, Microsoft Windows Server 2008 Datacenter Edition, Microsoft Windows Server 2008 Web Edition, Microsoft Windows Server 2008 HPC Edition, Microsoft Windows Server 2008 Storage Edition, Microsoft Windows Small Business Server 2008, Microsoft Windows Essential Business Server 2008
Disable NULL sessions for Windows 2008
Open Local Security Settings, and disable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Allow anonymous SID/Name translation: Disabled,
Network access: Let Everyone permissions apply to anonymous users : Disabled

Open Local Security Settings, and enable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Do not allow anonymous enumeration of SAM accounts: Enabled,
Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled,
Network access: Restrict anonymous access to Named Pipes and Shares: Enabled

Open Local Security Settings, and apply an empty list to the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Named Pipes that can be accessed anonymously,
Network access: Shares that can be accessed anonymously

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 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 Standard Edition, Microsoft Windows Vista Enterprise Edition, Microsoft Windows Vista Business Edition, Microsoft Windows Vista Business N Edition, Microsoft Windows Vista Start Edition
Disable NULL sessions for Windows Vista
Open Local Security Settings from Administrative Tools, and disable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Allow anonymous SID/Name translation: Disabled,
Network access: Let Everyone permissions apply to anonymous users : Disabled

Open Local Security Settings, and enable the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Do not allow anonymous enumeration of SAM accounts: Enabled,
Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled,
Network access: Restrict anonymous access to Named Pipes and Shares: Enabled

Open Local Security Settings, and apply an empty list to the following settings:

Security Settings -> Local Policies -> Security Options ->
Network access: Named Pipes that can be accessed anonymously,
Network access: Shares that can be accessed anonymously

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 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 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.

3.1.45. 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:

Affected Nodes:	Additional Information:
10.0.2.4:139	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian
10.0.2.4:445	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
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.

3.1.46. 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:
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
BID	55522
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.

3.1.47. 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:
10.0.2.4:3306	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.

3.1.48. 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:
10.0.2.4:22	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

Source	Reference
URL	http://www.ubuntu.com/usn/usn-612-3
URL	http://www.ubuntu.com/usn/usn-612-4
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 recomended 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 recomended to install these upgrades on all systems.

3.1.49. PHP Vulnerability: CVE-2016-7126 (php-cve-2016-7126)

Description:

The imagetruecolortopalette function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate the number of colors, which allows remote attackers to cause a denial of service (select_colors allocation error and out-of-bounds write) or possibly have unspecified other impact via a large value in the third argument.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	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	92755
CVE	CVE-2016-7126

Source	Reference
REDHAT	RHSA-2016:2750

Vulnerability Solution:

•Upgrade to PHP version 5.6.25

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

•Upgrade to PHP version 7.0.10

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

3.1.50. PHP Vulnerability: CVE-2016-9138 (php-cve-2016-9138)

Description:

PHP through 5.6.27 and 7.x through 7.0.12 mishandles property modification during __wakeup processing, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data, as demonstrated by Exception::__toString with DateInterval::__wakeup.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	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	95268
CVE	CVE-2016-9138
URL	https://bugs.php.net/bug.php?id=73147

Vulnerability Solution:

•Upgrade to PHP version 5.6.27

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

•Upgrade to PHP version 7.0.12

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

3.1.51. '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:
10.0.2.4:513	Running Remote Login service

References:

Source	Reference
CVE	CVE-1999-0651

Vulnerability Solution:

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

3.1.52. '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:
10.0.2.4:514	Running Remote Shell service

References:

Source	Reference
CVE	CVE-1999-0651

Vulnerability Solution:

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

3.1.53. 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:
10.0.2.4	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	9417
REDHAT	RHSA-2010:0140
REDHAT	RHSA-2011:0180
REDHAT	RHSA-2011:0309
USN	1082-1
XF	64832
XF	65770

Vulnerability Solution:

•gir1.0-pango-1.0 on Ubuntu Linux

Upgrade gir1.0-pango-1.0

Use `apt-get upgrade` to upgrade gir1.0-pango-1.0 to the latest version.

•libpango1.0-0 on Ubuntu Linux

Upgrade libpango1.0-0

Use `apt-get upgrade` to upgrade libpango1.0-0 to the latest version.

3.1.54. 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:
10.0.2.4	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	12812
REDHAT	RHSA-2011:0428
REDHAT	RHSA-2011:0840
USN	1108-1
XF	66580

Vulnerability Solution:

dhcp3-client on Ubuntu Linux

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

3.1.55. 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:

Affected Nodes:	Additional Information:
10.0.2.4	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
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

Source	Reference
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	11939
OVAL	12528
OVAL	12569
REDHAT	RHSA-2011:1423
REDHAT	RHSA-2011:1741
REDHAT	RHSA-2012:0071
REDHAT	RHSA-2013:1307
REDHAT	RHSA-2013:1615
REDHAT	RHSA-2014:0311
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

Upgrade libapache2-mod-php5

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

•php-pear on Ubuntu Linux

Upgrade php-pear

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

•php5 on Ubuntu Linux

Upgrade php5

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

•php5-cgi on Ubuntu Linux

Upgrade php5-cgi

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

•php5-cli on Ubuntu Linux

Upgrade php5-cli

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

•php5-common on Ubuntu Linux

Upgrade php5-common

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

•php5-curl on Ubuntu Linux

Upgrade php5-curl

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

•php5-dev on Ubuntu Linux

Upgrade php5-dev

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

•php5-gd on Ubuntu Linux

Upgrade php5-gd

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

•php5-intl on Ubuntu Linux

Upgrade php5-intl

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

3.1.56. 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:
10.0.2.4	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	10114
OVAL	10760
OVAL	6756
OVAL	8542
REDHAT	RHSA-2010:0329
REDHAT	RHSA-2011:0918
USN	1158-1
XF	52405

Vulnerability Solution:

•libcurl3 on Ubuntu Linux

Upgrade libcurl3

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

•libcurl3-gnutls on Ubuntu Linux

Upgrade libcurl3-gnutls

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

•libcurl3-nss on Ubuntu Linux

Upgrade libcurl3-nss

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

3.1.57. 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:
10.0.2.4	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	14762
OVAL	14824
OVAL	18827
REDHAT	RHSA-2011:1245
REDHAT	RHSA-2011:1294
REDHAT	RHSA-2011:1300
REDHAT	RHSA-2011:1329
REDHAT	RHSA-2011:1330
REDHAT	RHSA-2011:1369

Source	Reference
USN	1199-1
XF	69396

Vulnerability Solution:

•apache2.2-bin on Ubuntu Linux

Upgrade apache2.2-bin

Use `apt-get upgrade` to upgrade apache2.2-bin to the latest version.

•apache2-mpm-event on Ubuntu Linux

Upgrade apache2-mpm-event

Use `apt-get upgrade` to upgrade apache2-mpm-event to the latest version.

•apache2-mpm-perchild on Ubuntu Linux

Upgrade apache2-mpm-perchild

Use `apt-get upgrade` to upgrade apache2-mpm-perchild to the latest version.

•apache2-mpm-prefork on Ubuntu Linux

Upgrade apache2-mpm-prefork

Use `apt-get upgrade` to upgrade apache2-mpm-prefork to the latest version.

•apache2-mpm-worker on Ubuntu Linux

Upgrade apache2-mpm-worker

Use `apt-get upgrade` to upgrade apache2-mpm-worker to the latest version.

3.1.58. 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:
10.0.2.4	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

Source	Reference
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
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	1231-1
XF	58587
XF	67606
XF	67999
XF	69319
XF	69320
XF	69428
XF	69430

Vulnerability Solution:

•libapache2-mod-php5 on Ubuntu Linux

Upgrade libapache2-mod-php5

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

•php5-cgi on Ubuntu Linux
Upgrade php5-cgi
Use `apt-get upgrade` to upgrade php5-cgi to the latest version.
•php5-cli on Ubuntu Linux
Upgrade php5-cli
Use `apt-get upgrade` to upgrade php5-cli to the latest version.
•php5-common on Ubuntu Linux
Upgrade php5-common
Use `apt-get upgrade` to upgrade php5-common to the latest version.

3.1.59. 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:
10.0.2.4	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

Source	Reference
CVE	CVE-2012-0830
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	1358-1
XF	66180
XF	72021
XF	72908
XF	72911
XF	73125

Vulnerability Solution:

•libapache2-mod-php5 on Ubuntu Linux

Upgrade libapache2-mod-php5

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

•php5 on Ubuntu Linux

Upgrade php5

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

•php5-cgi on Ubuntu Linux

Upgrade php5-cgi

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

•php5-cli on Ubuntu Linux

Upgrade php5-cli

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

•php5-common on Ubuntu Linux

Upgrade php5-common

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

•php5-xsl on Ubuntu Linux

Upgrade php5-xsl

Use `apt-get upgrade` to upgrade php5-xsl to the latest version.

3.1.60. 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:
10.0.2.4	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
CVE	CVE-2009-5063
CVE	CVE-2011-3026
OVAL	15032
USN	1367-1

Vulnerability Solution:

libpng12-0 on Ubuntu Linux

Use `apt-get upgrade` to upgrade libpng12-0 to the latest version.

3.1.61. 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:
10.0.2.4	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	1374-1
XF	73361

Vulnerability Solution:

samba on Ubuntu Linux

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

3.1.62. 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:
10.0.2.4	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
CVE	CVE-2011-1095
CVE	CVE-2011-1658
CVE	CVE-2011-1659
CVE	CVE-2011-2702

Source	Reference
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	12272
OVAL	12853
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	1396-1
XF	66819
XF	66820

Vulnerability Solution:

•libc-bin on Ubuntu Linux

Upgrade libc-bin

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

•libc6 on Ubuntu Linux

Upgrade libc6

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

3.1.63. 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:
10.0.2.4	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
REDHAT	RHSA-2012:0546
REDHAT	RHSA-2012:0547
REDHAT	RHSA-2012:0568
USN	1437-1

Vulnerability Solution:

php5-cgi on Ubuntu Linux

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

3.1.64. 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:

Affected Nodes:	Additional Information:
10.0.2.4	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
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	1498-1

Vulnerability Solution:

•libtiff-tools on Ubuntu Linux

Upgrade libtiff-tools

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

•libtiff4 on Ubuntu Linux

Upgrade libtiff4

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

3.1.65. 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:
10.0.2.4	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	19706
REDHAT	RHSA-2012:1363
REDHAT	RHSA-2012:1364
REDHAT	RHSA-2012:1365
USN	1601-1

Vulnerability Solution:

bind9 on Ubuntu Linux

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

3.1.66. 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 15.15.5 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:
10.0.2.4	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

Source	Reference
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
IAVM	2012-A-0153
OVAL	19446
REDHAT	RHSA-2011:1424
REDHAT	RHSA-2011:1797
REDHAT	RHSA-2013:0685
USN	1643-1
XF	80098

Vulnerability Solution:

perl on Ubuntu Linux

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

3.1.67. 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:
10.0.2.4	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

Source	Reference
BID	58311
CVE	CVE-2013-1667
DEBIAN	DSA-2641
OSVDB	90892
OVAL	18771
REDHAT	RHSA-2013:0685
USN	1770-1
XF	82598

Vulnerability Solution:

perl on Ubuntu Linux

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

3.1.68. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 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	612-2
XF	42375

Vulnerability Solution:

•openssh-client on Ubuntu Linux

Upgrade openssh-client

Use `apt-get upgrade` to upgrade openssh-client to the latest version.

•openssh-server on Ubuntu Linux

Upgrade openssh-server

Use `apt-get upgrade` to upgrade openssh-server to the latest version.

3.1.69. 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:
10.0.2.4	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	612-4
XF	42375

Vulnerability Solution:

ssl-cert on Ubuntu Linux

Use `apt-get upgrade` to upgrade ssl-cert to the latest version.

3.1.70. 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:
10.0.2.4	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	624-1

Vulnerability Solution:

libpcre3 on Ubuntu Linux

Use `apt-get upgrade` to upgrade libpcre3 to the latest version.

3.1.71. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04

Affected Nodes:	Additional Information:
	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	10270
OVAL	10968
OVAL	11567
OVAL	12237
OVAL	12321
OVAL	12473
REDHAT	RHSA-2009:1107
REDHAT	RHSA-2009:1108
USN	786-1
XF	50964

Vulnerability Solution:

libaprutil1 on Ubuntu Linux

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

3.1.72. 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:

Affected Nodes:	Additional Information:
10.0.2.4	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	10687
OVAL	6136
REDHAT	RHSA-2009:1116
USN	790-1
XF	50554

Vulnerability Solution:

libsasl2-2 on Ubuntu Linux

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

3.1.73. 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:
10.0.2.4	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	10763
OVAL	10778
OVAL	6631
OVAL	7155
OVAL	8409
OVAL	8594
REDHAT	RHSA-2009:1207
REDHAT	RHSA-2009:1232
REDHAT	RHSA-2009:1432
REDHAT	RHSA-2010:0095
USN	809-1
XF	52404

Vulnerability Solution:

•libgnutls13 on Ubuntu Linux

Upgrade libgnutls13

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

•libgnutls26 on Ubuntu Linux

Upgrade libgnutls26

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

3.1.74. 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:
10.0.2.4	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
IAVM	2011-A-0147
IAVM	2012-A-0148
IAVM	2012-A-0153
REDHAT	RHSA-2011:0412
USN	944-1
XF	41504
XF	58915
XF	59240

Vulnerability Solution:

libc6 on Ubuntu Linux

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

3.1.75. 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:
10.0.2.4	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	12427
OVAL	7115
OVAL	9859
REDHAT	RHSA-2010:0488
USN	951-1
XF	59481

Vulnerability Solution:

samba on Ubuntu Linux

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

3.1.76. 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:
10.0.2.4	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
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	11851
USN	960-1
XF	59815
XF	59816

Vulnerability Solution:

libpng12-0 on Ubuntu Linux

Use `apt-get upgrade` to upgrade libpng12-0 to the latest version.

3.1.77. 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:
10.0.2.4	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

Source	Reference
BID	43212
CVE	CVE-2010-3069
REDHAT	RHSA-2010:0860
USN	987-1
XF	61773

Vulnerability Solution:

samba on Ubuntu Linux

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

3.1.78. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu php5-cli 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-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

Source	Reference
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	989-1
XF	58585
XF	59610

Vulnerability Solution:

•libapache2-mod-php5 on Ubuntu Linux

Upgrade libapache2-mod-php5

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

•php5-cgi on Ubuntu Linux

Upgrade php5-cgi

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

•php5-cli on Ubuntu Linux

Upgrade php5-cli

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

3.1.79. .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:
10.0.2.4	The following .rhosts files were found./home/msfadmin/.rhosts (-rwx------)

Affected Nodes:	Additional Information:
	/root/.rhosts (-rwx------)

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: 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:
10.0.2.4:80	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	V0057381
DISA_VMSKEY	V0061101
IAVM	2014-A-0172
IAVM	2015-A-0149
REDHAT	RHSA-2014:1019
REDHAT	RHSA-2014:1020
REDHAT	RHSA-2014:1021

Source	Reference
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.

3.2.2. X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)

Description:

The subject common name (CN) field in the X.509 certificate does not match the name of the entity presenting the certificate.

Before issuing a certificate, a Certification Authority (CA) must check the identity of the entity requesting the certificate, as specified in the CA's Certification Practice Statement (CPS). Thus, standard certificate validation procedures require the subject CN field of a certificate to match the actual name of the entity presenting the certificate. For example, in a certificate presented by "https://www.example.com/", the CN should be "www.example.com".

In order to detect and prevent active eavesdropping attacks, the validity of a certificate must be verified, or else an attacker could then launch a man-in-the-middle attack and gain full control of the data stream. Of particular importance is the validity of the subject's CN, that should match the name of the entity (hostname).

A CN mismatch most often occurs due to a configuration error, though it can also indicate that a man-in-the-middle attack is being conducted.

Please note that this check may flag a false positive against servers that are properly configured using SNI.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:25	The subject common name found in the X.509 certificate does not seem to match the scan target:Subject CN ubuntu804-base.localdomain does not match

Affected Nodes:	Additional Information:
	target name specified in the site.Subject CN ubuntu804-base.localdomain could not be resolved to an IP address via DNS lookup
10.0.2.4:5432	The subject common name found in the X.509 certificate does not seem to match the scan target:Subject CN ubuntu804-base.localdomain does not match target name specified in the site.Subject CN ubuntu804-base.localdomain could not be resolved to an IP address via DNS lookup

References:

None

Vulnerability Solution:

The subject's common name (CN) field in the X.509 certificate should be fixed to reflect the name of the entity presenting the certificate (e.g., the hostname). This is done by generating a new certificate usually signed by a Certification Authority (CA) trusted by both the client and server.

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:
10.0.2.4:139	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian
10.0.2.4:445	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
OVAL	9758
REDHAT	RHSA-2007:0060
REDHAT	RHSA-2007:0061
SGI	20070201-01-P
SUSE	SUSE-SA:2007:016

Source	Reference
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:
10.0.2.4:139	SMB signing is disabled
10.0.2.4:445	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:
10.0.2.4:21	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. 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:
10.0.2.4	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.

3.2.7. 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:
10.0.2.4:3306	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	10940
OVAL	8510
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.

3.2.8. 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:
10.0.2.4:3306	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.

3.2.9. PHP Vulnerability: CVE-2015-8866 (php-cve-2015-8866)

Description:

ext/libxml/libxml.c in PHP before 5.5.22 and 5.6.x before 5.6.6, when PHP-FPM is used, does not isolate each thread from libxml_disable_entity_loader changes in other threads, which allows remote attackers to conduct XML External Entity (XXE) and XML Entity Expansion (XEE) attacks via a crafted XML document, a related issue to CVE-2015-5161.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	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	87470
CVE	CVE-2015-8866
REDHAT	RHSA-2016:2750
URL	http://www.php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=64938

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/

3.2.10. PHP Vulnerability: CVE-2016-3171 (php-cve-2016-3171)

Description:

Drupal 6.x before 6.38, when used with PHP before 5.4.45, 5.5.x before 5.5.29, or 5.6.x before 5.6.13, might allow remote attackers to execute arbitrary code via vectors related to session data truncation.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	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-2016-3171
DEBIAN	DSA-3498

Vulnerability Solution:

•Upgrade to PHP version 5.4.45

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

•Upgrade to PHP version 5.5.29

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

•Upgrade to PHP version 5.6.13

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

3.2.11. PHP Vulnerability: CVE-2016-5767 (php-cve-2016-5767)

Description:

Integer overflow in the gdImageCreate function in gd.c in the GD Graphics Library (aka libgd) before 2.0.34RC1, as used in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8, allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted image dimensions.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	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	91395
CVE	CVE-2016-5767
REDHAT	RHSA-2016:2598
REDHAT	RHSA-2016:2750

Vulnerability Solution:

•Upgrade to PHP version 5.5.37

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

•Upgrade to PHP version 5.6.23

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

3.2.12. PHP Vulnerability: CVE-2018-19520 (php-cve-2018-19520)

Description:

An issue was discovered in SDCMS 1.6 with PHP 5.x. app/admin/controller/themecontroller.php uses a check_bad function in an attempt to block certain PHP functions such as eval, but does not prevent use of preg_replace 'e' calls, allowing users to execute arbitrary code by leveraging access to admin template management.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	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-2018-19520

Vulnerability Solution:

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

3.2.13. PHP Vulnerability: CVE-2019-6977 (php-cve-2019-6977)

Description:

gdImageColorMatch in gd_color_match.c in the GD Graphics Library (aka LibGD) 2.2.5, as used in the imagecolormatch function in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1, has a heap-based buffer overflow. This can be exploited by an attacker who is able to trigger imagecolormatch calls with crafted image data.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	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	106731
CVE	CVE-2019-6977
DEBIAN	DSA-4384
REDHAT	RHSA-2019:2519

Source	Reference
REDHAT	RHSA-2019:3299
URL	https://bugs.php.net/bug.php?id=77270

Vulnerability Solution:

•Upgrade to PHP version 5.6.40

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

•Upgrade to PHP version 7.2.14

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

•Upgrade to PHP version 7.3.1

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

3.2.14. X.509 Server Certificate Is Invalid/Expired (tls-server-cert-expired)

Description:

The TLS/SSL server's X.509 certificate either contains a start date in the future or is expired. Please refer to the proof for more details.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:25	The certificate is not valid after Fri, 16 Apr 2010 10:07:45 EDT
10.0.2.4:5432	The certificate is not valid after Fri, 16 Apr 2010 10:07:45 EDT

References:

None

Vulnerability Solution:

Obtain a new certificate and install it on the server. The exact instructions for obtaining a new certificate depend on your organization's requirements. Generally, you will need to generate a certificate request and save the request as a file. This file is then sent to a Certificate Authority (CA) for processing. Please ensure that the start date and the end date on the new certificate are valid.

Your organization may have its own internal Certificate Authority. If not, you may have to pay for a certificate from a trusted external Certificate Authority.

After you have received a new certificate file from the Certificate Authority, you will have to install it on the TLS/SSL server. The exact instructions for installing a certificate differ for each product. Please follow their documentation.

3.2.15. 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:
10.0.2.4	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	1009-1

Vulnerability Solution:

libc6 on Ubuntu Linux

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

3.2.16. 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:
10.0.2.4	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-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	1042-1
XF	64470

Vulnerability Solution:

•libapache2-mod-php5 on Ubuntu Linux

Upgrade libapache2-mod-php5

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

•php5-cgi on Ubuntu Linux

Upgrade php5-cgi

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

•php5-cli on Ubuntu Linux

Upgrade php5-cli

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

3.2.17. 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:
10.0.2.4	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	1102-1
XF	66247

Vulnerability Solution:

libtiff4 on Ubuntu Linux

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

3.2.18. 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:
10.0.2.4	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	1113-1
XF	65932

Vulnerability Solution:

postfix on Ubuntu Linux

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

3.2.19. 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:
10.0.2.4	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	1131-1
XF	67359

Vulnerability Solution:

postfix on Ubuntu Linux

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

3.2.20. 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:
10.0.2.4	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

Source	Reference
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	1140-1
XF	49110
XF	65035
XF	65036

Vulnerability Solution:

libpam-modules on Ubuntu Linux

Use `apt-get upgrade` to upgrade libpam-modules to the latest version.

3.2.21. 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:
10.0.2.4	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

Source	Reference
CVE	CVE-2011-1155
CVE	CVE-2011-1548
REDHAT	RHSA-2011:0407
USN	1172-1

Vulnerability Solution:

logrotate on Ubuntu Linux

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

3.2.22. 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:
10.0.2.4	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
CVE	CVE-2011-2501
CVE	CVE-2011-2690
CVE	CVE-2011-2692
DEBIAN	DSA-2287
REDHAT	RHSA-2011:1103
REDHAT	RHSA-2011:1104

Source	Reference
REDHAT	RHSA-2011:1105
USN	1175-1
XF	68517
XF	68536
XF	68538

Vulnerability Solution:

libpng12-0 on Ubuntu Linux

Use `apt-get upgrade` to upgrade libpng12-0 to the latest version.

3.2.23. 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:
10.0.2.4	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	1237-1

Vulnerability Solution:

libpam-modules on Ubuntu Linux

Use `apt-get upgrade` to upgrade libpam-modules to the latest version.

3.2.24. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 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	1378-1

Vulnerability Solution:

•postgresql-8.3 on Ubuntu Linux

Upgrade postgresql-8.3

Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version.

•postgresql-8.4 on Ubuntu Linux

Upgrade postgresql-8.4

Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version.

•postgresql-9.1 on Ubuntu Linux

Upgrade postgresql-9.1

Use `apt-get upgrade` to upgrade postgresql-9.1 to the latest version.

3.2.25. USN-1402-1: libpng vulnerability (ubuntu-usn-1402-1)

Description:

Integer signedness error in the png_inflate function in pngrutil.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:
10.0.2.4	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	14763
REDHAT	RHSA-2012:0488
USN	1402-1

Vulnerability Solution:

libpng12-0 on Ubuntu Linux

Use `apt-get upgrade` to upgrade libpng12-0 to the latest version.

3.2.26. 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:
10.0.2.4	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

Source	Reference
DEBIAN	DSA-2447
DEBIAN	DSA-2552
OSVDB	81025
REDHAT	RHSA-2012:0468
USN	1416-1
XF	74656

Vulnerability Solution:

libtiff4 on Ubuntu Linux

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

3.2.27. 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:
10.0.2.4	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	1417-1
XF	74494

Vulnerability Solution:

libpng12-0 on Ubuntu Linux

Use `apt-get upgrade` to upgrade libpng12-0 to the latest version.

3.2.28. 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:
10.0.2.4	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	1442-1

Vulnerability Solution:

•sudo on Ubuntu Linux

Upgrade sudo

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

•sudo-ldap on Ubuntu Linux

Upgrade sudo-ldap

Use `apt-get upgrade` to upgrade sudo-ldap to the latest version.

3.2.29. 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:
10.0.2.4	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
REDHAT	RHSA-2013:0217
USN	1447-1

Vulnerability Solution:

libxml2 on Ubuntu Linux

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

3.2.30. 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:
10.0.2.4	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
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	1451-1
XF	75525

Vulnerability Solution:

•libssl0.9.8 on Ubuntu Linux

Upgrade libssl0.9.8

Use `apt-get upgrade` to upgrade libssl0.9.8 to the latest version.

•libssl1.0.0 on Ubuntu Linux

Upgrade libssl1.0.0

Use `apt-get upgrade` to upgrade libssl1.0.0 to the latest version.

•openssl on Ubuntu Linux

Upgrade openssl

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

3.2.31. 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:
10.0.2.4	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	1576-1

Vulnerability Solution:

•dbus on Ubuntu Linux

Upgrade dbus

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

•libdbus-1-3 on Ubuntu Linux

Upgrade libdbus-1-3

Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version.

3.2.32. 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:
10.0.2.4	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

Source	Reference
CVE	CVE-2012-2807
DEBIAN	DSA-2521
DISA_SEVERITY	Category I
DISA_VMSKEY	V0036787
IAVM	2013-A-0031
USN	1587-1

Vulnerability Solution:

libxml2 on Ubuntu Linux

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

3.2.33. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libc6 2.7-10ubuntu5

References:

Source	Reference
BID	54982
CVE	CVE-2012-3404
CVE	CVE-2012-3405
CVE	CVE-2012-3406
CVE	CVE-2012-3480
DISA_SEVERITY	Category I
DISA_VMSKEY	V0058753
IAVM	2015-A-0038
OSVDB	84710

Source	Reference
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	1589-1

Vulnerability Solution:

libc6 on Ubuntu Linux

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

3.2.34. 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:
10.0.2.4	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
APPLE	APPLE-SA-2015-12-08-3
BID	40370
BID	40863
BID	44533
BID	46541

Source	Reference
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
IAVM	2012-A-0020
IAVM	2012-A-0189
OVAL	12210
REDHAT	RHSA-2011:0027
REDHAT	RHSA-2012:0731
USN	1613-1

Vulnerability Solution:

•python2.5 on Ubuntu Linux

Upgrade python2.5

Use `apt-get upgrade` to upgrade python2.5 to the latest version.

•python2.5-minimal on Ubuntu Linux

Upgrade python2.5-minimal

Use `apt-get upgrade` to upgrade python2.5-minimal to the latest version.

3.2.35. 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:
10.0.2.4	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
DISA_SEVERITY	Category I
DISA_VMSKEY	V0036903
IAVM	2013-A-0048
OSVDB	86878
REDHAT	RHSA-2012:1590
USN	1631-1
XF	79750

Vulnerability Solution:

•libtiff4 on Ubuntu Linux

Upgrade libtiff4

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

•libtiff5 on Ubuntu Linux

Upgrade libtiff5

Use `apt-get upgrade` to upgrade libtiff5 to the latest version.

3.2.36. 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:
10.0.2.4	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	1655-1
XF	80339

Vulnerability Solution:

libtiff4 on Ubuntu Linux

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

3.2.37. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libxml2 2.6.31.dfsg-2ubuntu1

References:

Source	Reference

Source	Reference
APPLE	APPLE-SA-2013-09-18-2
APPLE	APPLE-SA-2013-10-22-8
BID	56684
CVE	CVE-2012-5134
DEBIAN	DSA-2580
REDHAT	RHSA-2012:1512
REDHAT	RHSA-2013:0217
USN	1656-1
XF	80294

Vulnerability Solution:

libxml2 on Ubuntu Linux

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

3.2.38. 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:
10.0.2.4	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	1717-1

Source	Reference
XF	81917

Vulnerability Solution:

•postgresql-8.3 on Ubuntu Linux

Upgrade postgresql-8.3

Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version.

•postgresql-8.4 on Ubuntu Linux

Upgrade postgresql-8.4

Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version.

•postgresql-9.1 on Ubuntu Linux

Upgrade postgresql-9.1

Use `apt-get upgrade` to upgrade postgresql-9.1 to the latest version.

3.2.39. 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:
10.0.2.4	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
APPLE	APPLE-SA-2015-08-13-2
CVE	CVE-2013-1775
DEBIAN	DSA-2642
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061337
IAVM	2015-A-0199
OSVDB	90677
REDHAT	RHSA-2013:1353
REDHAT	RHSA-2013:1701

Source	Reference
USN	1754-1

Vulnerability Solution:

•sudo on Ubuntu Linux

Upgrade sudo

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

•sudo-ldap on Ubuntu Linux

Upgrade sudo-ldap

Use `apt-get upgrade` to upgrade sudo-ldap to the latest version.

3.2.40. 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:
10.0.2.4	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	695-1
XF	47037

Vulnerability Solution:

login on Ubuntu Linux

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

3.2.41. 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:
10.0.2.4	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	10856
OVAL	6462
REDHAT	RHSA-2009:0267
USN	722-1

Vulnerability Solution:
sudo on Ubuntu Linux
Use `apt-get upgrade` to upgrade sudo to the latest version.

3.2.42. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libcurl3-gnutls 7.18.0-1ubuntu2

References:

Source	Reference

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
BID	33962
CVE	CVE-2009-0037
DEBIAN	DSA-1738
OVAL	11054
OVAL	6074
REDHAT	RHSA-2009:0341
USN	726-1
XF	49030

Vulnerability Solution:

•libcurl3 on Ubuntu Linux

Upgrade libcurl3

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

•libcurl3-gnutls on Ubuntu Linux

Upgrade libcurl3-gnutls

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

3.2.43. 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:
10.0.2.4	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	732-1
XF	49216

Vulnerability Solution:

dash on Ubuntu Linux

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

3.2.44. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu udev 117-8

References:

Source	Reference
BID	34536
BID	34539
CVE	CVE-2009-1185
CVE	CVE-2009-1186
DEBIAN	DSA-1772
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061073
IAVM	2015-A-0150
OVAL	10925
OVAL	5975
REDHAT	RHSA-2009:0427
SUSE	SUSE-SA:2009:020
SUSE	SUSE-SA:2009:025
USN	758-1

Vulnerability Solution:

udev on Ubuntu Linux

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

3.2.45. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu cron 3.0pl1-100ubuntu2

References:

Source	Reference
BID	18108
CVE	CVE-2006-2607
OVAL	10213
REDHAT	RHSA-2006:0539
SUSE	SUSE-SA:2006:027
USN	778-1
XF	26691

Vulnerability Solution:

cron on Ubuntu Linux

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

3.2.46. 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:
10.0.2.4	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	36314
CVE	CVE-2009-3229
CVE	CVE-2009-3230
CVE	CVE-2009-3231
DEBIAN	DSA-1900
OVAL	10166
USN	834-1

Vulnerability Solution:

postgresql-8.3 on Ubuntu Linux

Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version.

3.2.47. 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:
10.0.2.4	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	11099
USN	842-1

Vulnerability Solution:

wget on Ubuntu Linux
Use `apt-get upgrade` to upgrade wget to the latest version.

3.2.48. 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:
10.0.2.4	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	9358
REDHAT	RHSA-2010:0427
REDHAT	RHSA-2010:0428
REDHAT	RHSA-2010:0429
USN	876-1

Vulnerability Solution:

•postgresql-8.3 on Ubuntu Linux
Upgrade postgresql-8.3
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version.
•postgresql-8.4 on Ubuntu Linux
Upgrade postgresql-8.4
Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version.

3.2.49. USN-889-1: gzip vulnerabilities (ubuntu-usn-889-1)

Description:

Integer underflow in the unlzw function in unlzw.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 LZW compression, leading to an array index error.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4	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	10546
OVAL	7511
REDHAT	RHSA-2010:0061
REDHAT	RHSA-2010:0095
SUSE	SUSE-SA:2010:008
USN	889-1

Vulnerability Solution:

gzip on Ubuntu Linux

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

3.2.50. 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:
10.0.2.4	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	10814
OVAL	10946
OVAL	7216
OVAL	7238
USN	905-1

Vulnerability Solution:

•sudo on Ubuntu Linux

Upgrade sudo

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

•sudo-ldap on Ubuntu Linux

Upgrade sudo-ldap

Use `apt-get upgrade` to upgrade sudo-ldap to the latest version.

3.2.51. 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:

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

References:

Source	Reference
BID	37973
CVE	CVE-2010-0442
DEBIAN	DSA-2051
OVAL	9720
REDHAT	RHSA-2010:0427
REDHAT	RHSA-2010:0428
REDHAT	RHSA-2010:0429
USN	933-1
XF	55902

Vulnerability Solution:

•postgresql-8.3 on Ubuntu Linux

Upgrade postgresql-8.3

Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version.

•postgresql-8.4 on Ubuntu Linux

Upgrade postgresql-8.4

Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version.

3.2.52. 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:
10.0.2.4	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	10258
OVAL	10846
OVAL	6693
OVAL	7210
OVAL	7328
OVAL	9490
REDHAT	RHSA-2010:0442
REDHAT	RHSA-2010:0824
USN	950-1

Vulnerability Solution:

•mysql-server-5.0 on Ubuntu Linux

Upgrade mysql-server-5.0

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

•mysql-server-5.1 on Ubuntu Linux

Upgrade mysql-server-5.1

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

3.2.53. 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:
10.0.2.4	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	954-1

Vulnerability Solution:

libtiff4 on Ubuntu Linux

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

3.2.54. 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:
10.0.2.4	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

Source	Reference
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	963-1

Vulnerability Solution:

libfreetype6 on Ubuntu Linux

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

3.2.55. 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:
10.0.2.4	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	967-1

Vulnerability Solution:

w3m on Ubuntu Linux
Use `apt-get upgrade` to upgrade w3m to the latest version.

3.2.56. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libwww-perl 5.808-1

References:

Source	Reference
CVE	CVE-2010-2253
USN	981-1

Vulnerability Solution:
libwww-perl on Ubuntu Linux
Use `apt-get upgrade` to upgrade libwww-perl to the latest version.

3.2.57. 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:
10.0.2.4	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	982-1

Vulnerability Solution:

wget on Ubuntu Linux

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

3.2.58. 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:
10.0.2.4	Following entries in /etc/securetty may allow anonymous root logins: ttyS0tts/0 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 pts/53pts/54pts/55pts/56pts/57pts/58pts/59pts/60pts/61pts/62pts/63pts/64pts/65 pts/66pts/67pts/68pts/69pts/70pts/71pts/72pts/73pts/74pts/75pts/76pts/77pts/78 pts/79pts/80pts/81pts/82pts/83pts/84pts/85pts/86pts/87pts/88pts/89pts/90pts/91 pts/92pts/93pts/94pts/95pts/96pts/97pts/98pts/99pts/100pts/101pts/102pts/103 pts/104pts/105pts/106pts/107pts/108pts/109pts/110pts/111pts/112pts/113 pts/114pts/115pts/116pts/117pts/118pts/119pts/120pts/121pts/122pts/123 pts/124pts/125pts/126pts/127pts/128rshrlogin

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.

3.2.59. Apache HTTPD: Uninitialized memory reflection in mod_auth_digest (CVE-2017-9788) (apache-httpd-cve-2017-9788)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_auth_digest. Review your web server configuration for validation. The value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments. by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
BID	99569
CVE	CVE-2017-9788
DEBIAN	DSA-3913
REDHAT	RHSA-2017:2478
REDHAT	RHSA-2017:2479
REDHAT	RHSA-2017:2483
REDHAT	RHSA-2017:2708
REDHAT	RHSA-2017:2709
REDHAT	RHSA-2017:2710
REDHAT	RHSA-2017:3113
REDHAT	RHSA-2017:3114
REDHAT	RHSA-2017:3193
REDHAT	RHSA-2017:3194
REDHAT	RHSA-2017:3195
REDHAT	RHSA-2017:3239
REDHAT	RHSA-2017:3240
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 < 2.2.34

Upgrade to Apache HTTPD version 2.2.34

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.34.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 < 2.4.27

Upgrade to Apache HTTPD version 2.4.27

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.27.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.

3.2.60. CIFS Share Writeable By Guest (cifs-share-world-writeable)

Description:

A share was found which allows write access by the guest account or anonymously. 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:
10.0.2.4	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.

3.2.61. 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:
10.0.2.4:139	Smb signing is: disabled
10.0.2.4:445	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

3.2.62. SMB: Service supports deprecated SMBv1 protocol (cifs-smb1-deprecated)

Description:

The SMB1 protocol has been deprecated since 2014 and is considered obsolete and insecure.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:139	SMB1 is deprecated and should not be used

Affected Nodes:	Additional Information:
10.0.2.4:445	SMB1 is deprecated and should not be used

References:

Source	Reference
URL	https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

Vulnerability Solution:

•Samba

Remove/disable SMB1

For Samba systems on Linux, disabling SMB1 is quite straightforward:

How to configure Samba to use SMBv2 and disable SMBv1 on Linux or Unix

•Microsoft Windows

Remove/disable SMB1

For Windows 8.1 and Windows Server 2012 R2, removing SMB1 is trivial. On older OS'es it can't be removed but should be disabled.

This article contains system-specific details:

How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server

3.2.63. ISC BIND: Key algorithm rollover bug in bind9 (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:
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 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

Source	Reference
BID	45137
CERT-VN	837744
CVE	CVE-2010-3614
DEBIAN	DSA-2130
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.

3.2.64. 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 XMLDOM 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:
10.0.2.4:80	Running HTTP serviceHTTP TRACE request to http://10.0.2.4/ 1: TRACE / HTTP/1.1 2: Host: 10.0.2.4 3: Cookie: vulnerable=yes

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
BID	15222
BID	19915
BID	24456
BID	36956
BID	9506
CERT-VN	867593

Source	Reference
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	1445
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".

3.2.65. 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:
10.0.2.4:3306	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.

3.2.66. 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:
10.0.2.4:3306	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.

3.2.67. 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:
10.0.2.4:3306	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.

3.2.68. 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:
10.0.2.4:3306	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.

3.2.69. PHP Vulnerability: CVE-2016-3167 (php-cve-2016-3167)

Description:

Open redirect vulnerability in the drupal_goto function in Drupal 6.x before 6.38, when used with PHP before 5.4.7, allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a double-encoded URL in the "destination" parameter.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	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-2016-3167
DEBIAN	DSA-3498

Vulnerability Solution:

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

3.2.70. Untrusted TLS/SSL server X.509 certificate (tls-untrusted-ca)

Description:

The server's TLS/SSL certificate is signed by a Certification Authority (CA) that is not well-known or trusted. This could happen if: the chain/intermediate certificate is missing, expired or has been revoked; the server hostname does not match that configured in the certificate; the time/date is incorrect; or a self-signed certificate is being used. The use of a self-signed certificate is not recommended since it could indicate that a TLS/SSL man-in-the-middle attack is taking place

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
10.0.2.4:25	TLS/SSL certificate signed by unknown, untrusted CA: EMAILADDRESS=root@ubuntu804-base.localdomain, CN=ubuntu804-base.localdomain, OU=Office for Complication of Otherwise Simple Affairs, O=OCOSA, L=Everywhere, ST=There is no such thing outside US, C=XX -- [Path does not chain with any of the trust anchors].
10.0.2.4:5432	TLS/SSL certificate signed by unknown, untrusted CA: EMAILADDRESS=root@ubuntu804-base.localdomain, CN=ubuntu804-base.localdomain, OU=Office for Complication of Otherwise Simple Affairs, O=OCOSA, L=Everywhere, ST=There is no such thing outside US, C=XX -- [Path does not chain with any of the trust anchors].

References:

Source	Reference
URL	http://httpd.apache.org/docs/2.2/mod/mod_ssl.html
URL	http://nginx.org/en/docs/http/configuring_https_servers.html
URL	https://support.microsoft.com/en-us/kb/954755

Vulnerability Solution:

Ensure the common name (CN) reflects the name of the entity presenting the certificate (e.g., the hostname). If the certificate(s) or any of the chain certificate(s) have expired or been revoked, obtain a new certificate from your Certificate Authority (CA) by following their documentation. If a self-signed certificate is being used, consider obtaining a signed certificate from a CA.

References: Mozilla: Connection Untrusted ErrorSSLShopper: SSL Certificate Not Trusted ErrorWindows/IIS certificate chain config Apache SSL configNginx SSL configCertificateChain.io

3.2.71. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu fuse-utils 2.7.2-1ubuntu2

References:

Source	Reference
BID	44623

Source	Reference
CVE	CVE-2010-3879
OSVDB	70520
USN	1045-1
XF	62986

Vulnerability Solution:

fuse-utils on Ubuntu Linux

Use `apt-get upgrade` to upgrade fuse-utils to the latest version.

3.2.72. 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:
10.0.2.4	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	1307-1
XF	71612

Vulnerability Solution:

•php5-cgi on Ubuntu Linux

Upgrade php5-cgi

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

•php5-cli on Ubuntu Linux

Upgrade php5-cli

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

3.2.73. 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:
10.0.2.4	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
USN	1682-1
XF	80990

Vulnerability Solution:

•gnupg on Ubuntu Linux

Upgrade gnupg

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

•gnupg2 on Ubuntu Linux

Upgrade gnupg2

Use `apt-get upgrade` to upgrade gnupg2 to the latest version.

3.2.74. 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:
10.0.2.4	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	10033
REDHAT	RHSA-2008:0839
SUSE	SUSE-SA:2008:040
USN	636-1
XF	44460

Vulnerability Solution:
postfix on Ubuntu Linux
Use `apt-get upgrade` to upgrade postfix to the latest version.

3.2.75. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu openssl 0.9.8g-4ubuntu3

References:

Source	Reference

Source	Reference
APPLE	APPLE-SA-2009-05-12
BID	33150
CERT	TA09-133A
CVE	CVE-2008-5077
OVAL	6380
OVAL	9155
REDHAT	RHSA-2009:0004
USN	704-1

Vulnerability Solution:

•libssl0.9.8 on Ubuntu Linux

Upgrade libssl0.9.8

Use `apt-get upgrade` to upgrade libssl0.9.8 to the latest version.

•openssl on Ubuntu Linux

Upgrade openssl

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

3.2.76. 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:
10.0.2.4	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

Source	Reference
USN	953-1

Vulnerability Solution:

fastjar on Ubuntu Linux

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

3.2.77. 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:
10.0.2.4	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	10580
OVAL	7338
REDHAT	RHSA-2010:0475
USN	956-1

Vulnerability Solution:

•sudo on Ubuntu Linux

Upgrade sudo

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

•sudo-ldap on Ubuntu Linux

Upgrade sudo-ldap

Use `apt-get upgrade` to upgrade sudo-ldap to the latest version.

3.2.78. 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:
10.0.2.4	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
DEBIAN	DSA-3253
DISA_SEVERITY	Category I
DISA_VMSKEY	V0027158
IAVM	2011-A-0066
MS	MS10-049
OSVDB	60521
OSVDB	60972
OSVDB	62210

Source	Reference
OSVDB	65202
OVAL	10088
OVAL	11578
OVAL	11617
OVAL	7315
OVAL	7478
OVAL	7973
OVAL	8366
OVAL	8535
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	990-2
XF	54158

Vulnerability Solution:

apache2.2-common on Ubuntu Linux

Use `apt-get upgrade` to upgrade apache2.2-common to the latest version.

3.2.79. /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:
10.0.2.4	/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

3.2.80. 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 or ProxyPassMatch, 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 https://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	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
DEBIAN	DSA-2405
REDHAT	RHSA-2011:1391

Source	Reference
REDHAT	RHSA-2011:1392
REDHAT	RHSA-2012:0542
REDHAT	RHSA-2012:0543
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.

3.2.81. 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:
10.0.2.4:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8

Affected Nodes:	Additional Information:
	Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
APPLE	APPLE-SA-2015-09-16-4
BID	66550
CVE	CVE-2013-5704
REDHAT	RHSA-2015:0325
REDHAT	RHSA-2015:1249
REDHAT	RHSA-2015:2659
REDHAT	RHSA-2015:2660
REDHAT	RHSA-2015:2661
REDHAT	RHSA-2016:0061
REDHAT	RHSA-2016:0062
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.

3.2.82. 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:
10.0.2.4:80	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	V0057381
DISA_VMSKEY	V0061101
IAVM	2014-A-0172
IAVM	2015-A-0149
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 HTTPD: HTTP request smuggling attack against chunked request parser (CVE-2015-3183) (apache-httpd-cve-2015-3183)

Description:

An HTTP request smuggling attack was possible due to a bug in parsing of chunked requests. A malicious client could force the server to misinterpret the request length, allowing cache poisoning or credential hijacking if an intermediary proxy is in use.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	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-2015-08-13-2
APPLE	APPLE-SA-2015-09-16-4
BID	75963
BID	91787
CVE	CVE-2015-3183
DEBIAN	DSA-3325
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061135
DISA_VMSKEY	V0061337
IAVM	2015-A-0174
IAVM	2015-A-0199
REDHAT	RHSA-2015:1666
REDHAT	RHSA-2015:1667
REDHAT	RHSA-2015:1668
REDHAT	RHSA-2015:2659
REDHAT	RHSA-2015:2660
REDHAT	RHSA-2015:2661
REDHAT	RHSA-2016:0061
REDHAT	RHSA-2016:0062
REDHAT	RHSA-2016:2054

Source	Reference
REDHAT	RHSA-2016:2055
REDHAT	RHSA-2016:2056
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 < 2.2.31

Upgrade to Apache HTTPD version 2.2.31

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.31.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 < 2.4.16

Upgrade to Apache HTTPD version 2.4.16

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.16.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.

3.2.84. Apache HTTPD: HTTP_PROXY environment variable "httpoxy" mitigation (CVE-2016-5387) (apache-httpd-cve-2016-5387)

Description:

HTTP_PROXY is a well-defined environment variable in a CGI process, which collided with a number of libraries which failed to avoid colliding with this CGI namespace. A mitigation is provided for the httpd CGI environment to avoid populating the "HTTP_PROXY" variable from a "Proxy:" header, which has never been registered by IANA. This workaround and patch are documented in the ASF Advisory at asf-httpoxy-response.txt and incorporated in the 2.4.25 and 2.2.32 releases. Note: This is not assigned an httpd severity, as it is a defect in other software which overloaded well-established CGI environment variables, and does not reflect an error in HTTP server software.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
BID	91816

Source	Reference
CERT-VN	797896
CVE	CVE-2016-5387
DEBIAN	DSA-3623
DISA_SEVERITY	Category I
IAVM	2016-B-0160
IAVM	2017-A-0010
REDHAT	RHSA-2016:1420
REDHAT	RHSA-2016:1421
REDHAT	RHSA-2016:1422
REDHAT	RHSA-2016:1624
REDHAT	RHSA-2016:1625
REDHAT	RHSA-2016:1635
REDHAT	RHSA-2016:1636
REDHAT	RHSA-2016:1648
REDHAT	RHSA-2016:1649
REDHAT	RHSA-2016:1650
REDHAT	RHSA-2016:1851
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 < 2.2.32

Upgrade to Apache HTTPD version 2.2.32

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.32.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 < 2.4.25

Upgrade to Apache HTTPD version 2.4.25

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.25.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.

3.2.85. Apache HTTPD: Apache HTTP Request Parsing Whitespace Defects (CVE-2016-8743) (apache-httpd-cve-2016-8743)

Description:

Apache HTTP Server, prior to release 2.4.25 (2.2.32), accepted a broad pattern of unusual whitespace patterns from the user-agent, including bare CR, FF, VTAB in parsing the request line and request header lines, as well as HTAB in parsing the request line. Any bare CR present in request lines was treated as whitespace and remained in the request field member "the_request", while a bare CR in the request header field name would be honored as whitespace, and a bare CR in the request header field value was retained the input headers array. Implied additional whitespace was accepted in the request line and prior to the ':' delimiter of any request header lines. RFC7230 Section 3.5 calls out some of these whitespace exceptions, and section 3.2.3 eliminated and clarified the role of implied whitespace in the grammer of this specification. Section 3.1.1 requires exactly one single SP between the method and request-target, and between the request-target and HTTP-version, followed immediately by a CRLF sequence. None of these fields permit any (unencoded) CTL character whatsoever. Section 3.2.4 explicitly disallowed any whitespace from the request header field prior to the ':' character, while Section 3.2 disallows all CTL characters in the request header line other than the HTAB character as whitespace. These defects represent a security concern when httpd is participating in any chain of proxies or interacting with back-end application servers, either through mod_proxy or using conventional CGI mechanisms. In each case where one agent accepts such CTL characters and does not treat them as whitespace, there is the possiblity in a proxy chain of generating two responses from a server behind the uncautious proxy agent. In a sequence of two requests, this results in request A to the first proxy being interpreted as requests A + A' by the backend server, and if requests A and B were submitted to the first proxy in a keepalive connection, the proxy may interpret response A' as the response to request B, polluting the cache or potentially serving the A' content to a different downstream user-agent. These defects are addressed with the release of Apache HTTP Server 2.4.25 and coordinated by a new directive; HttpProtocolOptions Strict which is the default behavior of 2.4.25 and later. By toggling from 'Strict' behavior to 'Unsafe' behavior, some of the restrictions may be relaxed to allow some invalid HTTP/1.1 clients to communicate with the server, but this will reintroduce the possibility of the problems described in this assessment. Note that relaxing the behavior to 'Unsafe' will still not permit raw CTLs other than HTAB (where permitted), but will allow other RFC requirements to not be enforced, such as exactly two SP characters in the request line.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
BID	95077
CVE	CVE-2016-8743
DEBIAN	DSA-3796
DISA_SEVERITY	Category I
IAVM	2017-A-0010
REDHAT	RHSA-2017:0906
REDHAT	RHSA-2017:1161
REDHAT	RHSA-2017:1413
REDHAT	RHSA-2017:1414

Source	Reference
REDHAT	RHSA-2017:1415
REDHAT	RHSA-2017:1721
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 < 2.2.32

Upgrade to Apache HTTPD version 2.2.32

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.32.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 < 2.4.25

Upgrade to Apache HTTPD version 2.4.25

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.25.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.

3.2.86. Apache HTTPD: Use-after-free when using <Limit > with an unrecognized method in .htaccess ("OptionsBleed") (CVE-2017-9798) (apache-httpd-cve-2017-9798)

Description:

When an unrecognized HTTP Method is given in an <Limit {method}> directive in an .htaccess file, and that .htaccess file is processed by the corresponding request, the global methods table is corrupted in the current worker process, resulting in erratic behaviour. This behavior may be avoided by listing all unusual HTTP Methods in a global httpd.conf RegisterHttpMethod directive in httpd release 2.4.25 and later. To permit other .htaccess directives while denying the <Limit > directive, see the AllowOverrideList directive. Source code patch (2.4) is at; CVE-2017-9798-patch-2.4.patch Source code patch (2.2) is at; CVE-2017-9798-patch-2.2.patch Note 2.2 is end-of-life, no further release with this fix is planned. Users are encouraged to migrate to 2.4.28 or later for this and other fixes.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
BID	100872

Source	Reference
BID	105598
CVE	CVE-2017-9798
DEBIAN	DSA-3980
REDHAT	RHSA-2017:2882
REDHAT	RHSA-2017:2972
REDHAT	RHSA-2017:3018
REDHAT	RHSA-2017:3113
REDHAT	RHSA-2017:3114
REDHAT	RHSA-2017:3193
REDHAT	RHSA-2017:3194
REDHAT	RHSA-2017:3195
REDHAT	RHSA-2017:3239
REDHAT	RHSA-2017:3240
REDHAT	RHSA-2017:3475
REDHAT	RHSA-2017:3476
REDHAT	RHSA-2017:3477
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.28
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.28.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.

3.2.87. 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:
10.0.2.4:8180	Running HTTP serviceProduct Tomcat exists -- Apache TomcatHTTP GET request to http://10.0.2.4:8180/ HTTP response code was an expected 200 190: <td style="width:20px"> </td> 191: 192: <!-- Body --> 193: <td align="left" valign="top"> 194: ... means you've setup Tomcat successfully. Congratulations!</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.

3.2.88. 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:
10.0.2.4:139	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian
10.0.2.4:445	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

Source	Reference
DEBIAN	DSA-1110
OVAL	11355
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.

3.2.89. Database Open Access (database-open-access)

Description:

The database allows any remote system the ability to connect to it. It is recommended to limit direct access to trusted systems because databases may contain sensitive data, and new vulnerabilities and exploits are discovered routinely for them. For this reason, it is a violation of PCI DSS section 1.3.6 to have databases listening on ports accessible from the Internet, even when protected with secure authentication mechanisms.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:3306	Running MySQL service
10.0.2.4:5432	Running Postgres service

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

Vulnerability Solution:

Configure the database server to only allow access to trusted systems. For example, the PCI DSS standard requires you to place the database in an internal network zone, segregated from the DMZ

3.2.90. 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:
10.0.2.4:53	Received 1 answers to a non-recursive query for www.rapid7.com
10.0.2.4:53	Received 1 answers to a non-recursive query for www.rapid7.com

References:

Source	Reference
URL	http://cs.unc.edu/~fabian/course_papers/cache_snooping.pdf

Vulnerability Solution:

Restrict the processing of DNS queries to only systems that should be allowed to use this nameserver.

3.2.91. 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:
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 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
CERT-VN	606539

Source	Reference
CVE	CVE-2011-4313
DEBIAN	DSA-2347
OVAL	14343
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:

•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

•Upgrade ISC BIND to latest version

More information about upgrading your version of ISC BIND is available on the ISC website.

3.2.92. 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:
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 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
REDHAT	RHSA-2012:0717
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.

3.2.93. 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:
10.0.2.4:53	Nameserver resolved www.google.com to:www.google.com. 300 IN A 172.217.0.36
10.0.2.4:53	Nameserver resolved www.google.com to:www.google.com. 300 IN A 172.217.0.36

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.

3.2.94. 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:
10.0.2.4:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8HTTP GET request to http://10.0.2.4/doc/ HTTP response code was an expected 200 1: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"> 2: <html> 3: <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>

3.2.95. 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:
10.0.2.4:80	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

3.2.96. 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:
10.0.2.4:80	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	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

3.2.97. 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:
10.0.2.4	Grub config with no password found.Vulnerable file: /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/grub.cfg
/boot/grub/menu.lst

For all files mentioned above ensure that a password is set or that the files do not exist.
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.

3.2.98. 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:
10.0.2.4:40935	/
10.0.2.4:54020	/

References:

None

Vulnerability Solution:

Restrict mounting privileges to only hosts that require them.

3.2.99. 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:
10.0.2.4:80	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

3.2.100. 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:
10.0.2.4:80	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
XF	45956

Vulnerability Solution:
Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.6.tar.gz

3.2.101. 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:
10.0.2.4:80	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
OVAL	9667
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

3.2.102. 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:
10.0.2.4:80	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

3.2.103. 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:
10.0.2.4:80	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/

3.2.104. 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:
10.0.2.4:80	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/

3.2.105. 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:
10.0.2.4:80	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	72530
CVE	CVE-2013-6501

Vulnerability Solution:

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

3.2.106. PHP Vulnerability: CVE-2015-8867 (php-cve-2015-8867)

Description:

The openssl_random_pseudo_bytes function in ext/openssl/openssl.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 incorrectly relies on the deprecated RAND_pseudo_bytes function, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	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-2015-8867
REDHAT	RHSA-2016:2750
URL	http://www.php.net/ChangeLog-5.php
URL	http://www.php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=70014

Vulnerability Solution:

•Upgrade to PHP version 5.4.44

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

•Upgrade to PHP version 5.5.28

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

•Upgrade to PHP version 5.6.12

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

3.2.107. PHP Vulnerability: CVE-2015-8879 (php-cve-2015-8879)

Description:

The odbc_bindcols function in ext/odbc/php_odbc.c in PHP before 5.6.12 mishandles driver behavior for SQL_WVARCHAR columns, which allows remote attackers to cause a denial of service (application crash) in opportunistic circumstances by leveraging use of the odbc_fetch_array function to access a certain type of Microsoft SQL Server table.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	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-2015-8879
REDHAT	RHSA-2016:2750

Vulnerability Solution:

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

3.2.108. 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:
10.0.2.4:80	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
OVAL	9667
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

3.2.109. 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:
10.0.2.4:80	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

3.2.110. Postfix vulnerability (CVE-2017-10140) (postfix-cve-2017-10140)

Description:

Postfix before 2.11.10, 3.0.x before 3.0.10, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 might allow local users to gain privileges by leveraging undocumented functionality in Berkeley DB 2.x and later, related to reading settings from DB_CONFIG in the current directory.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:25	Running SMTP serviceProduct Postfix exists -- Postfix 2.5.1Vulnerable version of product Postfix found -- Postfix 2.5.1

References:

Source	Reference
CVE	CVE-2017-10140
REDHAT	RHSA-2019:0366

Vulnerability Solution:

For more information or to download Postfix updates, visit the Postfix website.

3.2.111. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 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

Source	Reference
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	11869
REDHAT	RHSA-2010:0824
REDHAT	RHSA-2010:0825
REDHAT	RHSA-2011:0164
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

Upgrade mysql-server-5.0

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

•mysql-server-5.1 on Ubuntu Linux

Upgrade mysql-server-5.1

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

3.2.112. 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:
10.0.2.4	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	11683
OVAL	12341
OVAL	12800
REDHAT	RHSA-2010:0659
REDHAT	RHSA-2010:0950
REDHAT	RHSA-2011:0896
REDHAT	RHSA-2011:0897
USN	1021-1

Vulnerability Solution:

apache2.2-common on Ubuntu Linux

Use `apt-get upgrade` to upgrade apache2.2-common to the latest version.

3.2.113. 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:
10.0.2.4	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	12800
REDHAT	RHSA-2010:0950
REDHAT	RHSA-2011:0896
REDHAT	RHSA-2011:0897
USN	1022-1

Vulnerability Solution:

libaprutil1 on Ubuntu Linux

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

3.2.114. 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:
10.0.2.4	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	1075-1
XF	65724

Vulnerability Solution:

samba on Ubuntu Linux

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

3.2.115. 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:
10.0.2.4	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

Source	Reference
REDHAT	RHSA-2011:1378
REDHAT	RHSA-2011:1423
SUSE	SUSE-SA:2011:035
USN	1229-1
XF	69319

Vulnerability Solution:

•postgresql-8.3 on Ubuntu Linux

Upgrade postgresql-8.3

Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version.

•postgresql-8.4 on Ubuntu Linux

Upgrade postgresql-8.4

Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version.

3.2.116. 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:
10.0.2.4	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

Source	Reference
CVE	CVE-2011-3368
DEBIAN	DSA-2202
OSVDB	76079
OVAL	14941
OVAL	18154
REDHAT	RHSA-2011:1391
REDHAT	RHSA-2011:1392
USN	1259-1
XF	66248
XF	69804
XF	70336

Vulnerability Solution:

•apache2.2-bin on Ubuntu Linux

Upgrade apache2.2-bin

Use `apt-get upgrade` to upgrade apache2.2-bin to the latest version.

•apache2.2-common on Ubuntu Linux

Upgrade apache2.2-common

Use `apt-get upgrade` to upgrade apache2.2-common to the latest version.

•apache2-mpm-itk on Ubuntu Linux

Upgrade apache2-mpm-itk

Use `apt-get upgrade` to upgrade apache2-mpm-itk to the latest version.

3.2.117. 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:
10.0.2.4	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	1308-1

Vulnerability Solution:

bzip2 on Ubuntu Linux

Use `apt-get upgrade` to upgrade bzip2 to the latest version.

3.2.118. 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:
10.0.2.4	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
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	1368-1
XF	71093

Vulnerability Solution:

apache2.2-common on Ubuntu Linux

Use `apt-get upgrade` to upgrade apache2.2-common to the latest version.

3.2.119. 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:
10.0.2.4	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	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	1376-1

Vulnerability Solution:

libxml2 on Ubuntu Linux

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

3.2.120. 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:
10.0.2.4	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	1418-1

Vulnerability Solution:

•libgnutls13 on Ubuntu Linux

Upgrade libgnutls13

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

•libgnutls26 on Ubuntu Linux

Upgrade libgnutls26

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

3.2.121. 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:
10.0.2.4	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	1436-1

Vulnerability Solution:

libtasn1-3 on Ubuntu Linux

Use `apt-get upgrade` to upgrade libtasn1-3 to the latest version.

3.2.122. 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:
10.0.2.4	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
BID	53911
CVE	CVE-2012-2122
USN	1467-1

Vulnerability Solution:

•mysql-server-5.0 on Ubuntu Linux

Upgrade mysql-server-5.0

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

•mysql-server-5.1 on Ubuntu Linux

Upgrade mysql-server-5.1

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

•mysql-server-5.5 on Ubuntu Linux

Upgrade mysql-server-5.5

Use `apt-get upgrade` to upgrade mysql-server-5.5 to the latest version.

3.2.123. 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:
10.0.2.4	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
APPLE	APPLE-SA-2015-12-08-3
BID	52379

Source	Reference
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	1527-1

Vulnerability Solution:

•lib64expat1 on Ubuntu Linux

Upgrade lib64expat1

Use `apt-get upgrade` to upgrade lib64expat1 to the latest version.

•libexpat1 on Ubuntu Linux

Upgrade libexpat1

Use `apt-get upgrade` to upgrade libexpat1 to the latest version.

•libexpat1-udeb on Ubuntu Linux

Upgrade libexpat1-udeb

Use `apt-get upgrade` to upgrade libexpat1-udeb to the latest version.

3.2.124. 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:
10.0.2.4	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

Source	Reference
BID	55072
BID	55074
CVE	CVE-2012-3488
CVE	CVE-2012-3489
DEBIAN	DSA-2534
REDHAT	RHSA-2012:1263
REDHAT	RHSA-2012:1264
USN	1542-1

Vulnerability Solution:

•postgresql-8.3 on Ubuntu Linux

Upgrade postgresql-8.3

Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version.

•postgresql-8.4 on Ubuntu Linux

Upgrade postgresql-8.4

Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version.

•postgresql-9.1 on Ubuntu Linux

Upgrade postgresql-9.1

Use `apt-get upgrade` to upgrade postgresql-9.1 to the latest version.

3.2.125. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libgc1c2 1:6.8-1.1

References:

Source	Reference
BID	54227

Source	Reference
CVE	CVE-2012-2673
REDHAT	RHSA-2013:1500
REDHAT	RHSA-2014:0149
REDHAT	RHSA-2014:0150
USN	1546-1

Vulnerability Solution:

libgc1c2 on Ubuntu Linux

Use `apt-get upgrade` to upgrade libgc1c2 to the latest version.

3.2.126. 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:
10.0.2.4	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	18754
OVAL	18841

Source	Reference
OVAL	18868
OVAL	19016
OVAL	19081
OVAL	19360
OVAL	19424
OVAL	19487
OVAL	19540
OVAL	19608
OVAL	19660
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	1732-1

Vulnerability Solution:

•libssl0.9.8 on Ubuntu Linux

Upgrade libssl0.9.8

Use `apt-get upgrade` to upgrade libssl0.9.8 to the latest version.

•libssl1.0.0 on Ubuntu Linux

Upgrade libssl1.0.0

Use `apt-get upgrade` to upgrade libssl1.0.0 to the latest version.

3.2.127. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04

Affected Nodes:	Additional Information:
	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	V0061101
IAVM	2015-A-0149
OVAL	18938
OVAL	18977
OVAL	19284
OVAL	19312
REDHAT	RHSA-2013:0815
REDHAT	RHSA-2013:1207
REDHAT	RHSA-2013:1208
REDHAT	RHSA-2013:1209
USN	1765-1

Vulnerability Solution:

apache2.2-common on Ubuntu Linux

Use `apt-get upgrade` to upgrade apache2.2-common to the latest version.

3.2.128. 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:
10.0.2.4	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	1801-1

Vulnerability Solution:

•curl on Ubuntu Linux

Upgrade curl

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

•libcurl3 on Ubuntu Linux

Upgrade libcurl3

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

3.2.129. 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:
10.0.2.4	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	10253
OVAL	9353
REDHAT	RHSA-2008:0159
REDHAT	RHSA-2009:0008
USN	653-1
XF	45701

Vulnerability Solution:

libdbus-1-3 on Ubuntu Linux

Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version.

3.2.130. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 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

Source	Reference
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	10133
OVAL	10521
OVAL	10591
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	671-1
XF	42267
XF	45042
XF	45648
XF	45649

Vulnerability Solution:

mysql-server-5.0 on Ubuntu Linux

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

3.2.131. 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:

Affected Nodes:	Additional Information:
10.0.2.4	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	8556
OVAL	9664
REDHAT	RHSA-2009:1463
USN	837-1

Vulnerability Solution:

libnewt0.52 on Ubuntu Linux

Use `apt-get upgrade` to upgrade libnewt0.52 to the latest version.

3.2.132. 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:
10.0.2.4	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

Source	Reference
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	10613
OVAL	11019
OVAL	12719
OVAL	12942
OVAL	6883
OVAL	7112
OVAL	8520
OVAL	9356
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	890-1

Vulnerability Solution:

•lib64expat1 on Ubuntu Linux

Upgrade lib64expat1

Use `apt-get upgrade` to upgrade lib64expat1 to the latest version.

•libexpat1 on Ubuntu Linux

Upgrade libexpat1

Use `apt-get upgrade` to upgrade libexpat1 to the latest version.

•libexpat1-udeb on Ubuntu Linux

Upgrade libexpat1-udeb

Use `apt-get upgrade` to upgrade libexpat1-udeb to the latest version.

3.2.133. 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:
10.0.2.4	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
USN	986-1

Vulnerability Solution:

•bzip2 on Ubuntu Linux

Upgrade bzip2

Use `apt-get upgrade` to upgrade bzip2 to the latest version.

•libbz2-1.0 on Ubuntu Linux

Upgrade libbz2-1.0

Use `apt-get upgrade` to upgrade libbz2-1.0 to the latest version.

3.2.134. 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:
10.0.2.4	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	986-3

Vulnerability Solution:

dpkg on Ubuntu Linux

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

3.2.135. Apache HTTPD: Potential pattern expansion problem when mod-proxy and mod-rewrite are used together (CVE-2011-3639) (apache-httpd-cve-2011-3639)

Description:

The affected asset is vulnerable to this vulnerability ONLY if proxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character. Review your web server configuration for validation.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
CVE	CVE-2011-3639
DEBIAN	DSA-2405
REDHAT	RHSA-2012:0128

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 < 2.2.18

Upgrade to Apache HTTPD version 2.2.18

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.18.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.

3.2.136. 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:
10.0.2.4:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8

Affected Nodes:	Additional Information:
	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	V0057381
DISA_VMSKEY	V0061101
IAVM	2014-A-0172
IAVM	2015-A-0149
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.

3.2.137. Apache HTTPD: mod_userdir CRLF injection (CVE-2016-4975) (apache-httpd-cve-2016-4975)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_userdir. Review your web server configuration for validation. Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
BID	105093
CVE	CVE-2016-4975
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 < 2.2.32

Upgrade to Apache HTTPD version 2.2.32

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.32.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 < 2.4.25

Upgrade to Apache HTTPD version 2.4.25

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.25.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.

3.2.138. ISC BIND: BIND 9 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:
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 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
OVAL	12205
OVAL	7212
OVAL	7430
OVAL	9357
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.

3.2.139. ISC BIND: Cache incorrectly allows a ncache entry and a 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:
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 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
OVAL	12601
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.

3.2.140. ISC BIND: A query name which is too long can cause a segmentation fault in lwresd (CVE-2016-2775) (dns-bind-cve-2016-2775)

Description:

ISC BIND 9.x before 9.9.9-P2, 9.10.x before 9.10.4-P2, and 9.11.x before 9.11.0b2, when lwresd or the named lwres option is enabled, allows remote attackers to cause a denial of service (daemon crash) via a long request that uses the lightweight resolver protocol.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2

References:

Source	Reference
BID	92037
CVE	CVE-2016-2775
DISA_SEVERITY	Category I
IAVM	2017-A-0004
REDHAT	RHBA-2017:0651
REDHAT	RHBA-2017:1767
REDHAT	RHSA-2017:2533
URL	https://kb.isc.org/article/AA-01393/0

Vulnerability Solution:

More information about upgrading your version of ISC BIND is available on the ISC website.

3.2.141. 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:
10.0.2.4:3306	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.

3.2.142. 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:
10.0.2.4:3306	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.

3.2.143. 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:
10.0.2.4:3306	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.

3.2.144. 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:
10.0.2.4:3306	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
DEBIAN	DSA-2429
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.

3.2.145. 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:
10.0.2.4:3306	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
DEBIAN	DSA-2429
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.

3.2.146. 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:
10.0.2.4:3306	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
DEBIAN	DSA-2429
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.

3.2.147. 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:
10.0.2.4:3306	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
DEBIAN	DSA-2429
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.

3.2.148. 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:
10.0.2.4:3306	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
DEBIAN	DSA-2429
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.

3.2.149. 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:
10.0.2.4:80	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-2008-03-18
BID	26403
CVE	CVE-2007-4887
OVAL	5767

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

3.2.150. 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:
10.0.2.4:80	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

Source	Reference
XF	37227

Vulnerability Solution:

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

3.2.151. 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:
10.0.2.4:80	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
DEBIAN	DSA-2398
DISA_SEVERITY	Category I
DISA_VMSKEY	V0031054

Source	Reference
IAVM	2012-B-0006
MS	MS12-006
OVAL	14752
REDHAT	RHSA-2011:1384
REDHAT	RHSA-2012:0006
REDHAT	RHSA-2012:0508
REDHAT	RHSA-2013:1455

Vulnerability Solution:

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

3.2.152. PHP Vulnerability: CVE-2017-7890 (php-cve-2017-7890)

Description:

The GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.31 and 7.x before 7.1.7, does not zero colorMap arrays before use. A specially crafted GIF image could use the uninitialized tables to read ~700 bytes from the top of the stack, potentially disclosing sensitive information.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	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	99492
CVE	CVE-2017-7890
DEBIAN	DSA-3938
REDHAT	RHSA-2018:0406
REDHAT	RHSA-2018:1296
URL	https://bugs.php.net/bug.php?id=74435
URL	https://bugs.php.net/patch-display.php?bug=74435&patch=fix-74435-php-7.0&revision=1497970038

Vulnerability Solution:

•Upgrade to PHP version 5.6.31

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

•Upgrade to PHP version 7.0.21

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

•Upgrade to PHP version 7.1.7

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

3.2.153. PHP Vulnerability: CVE-2018-17082 (php-cve-2018-17082)

Description:

The Apache2 component in PHP before 5.6.38, 7.0.x before 7.0.32, 7.1.x before 7.1.22, and 7.2.x before 7.2.10 allows XSS via the body of a "Transfer-Encoding: chunked" request, because the bucket brigade is mishandled in the php_handler function in sapi/apache2handler/sapi_apache2.c.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	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-2018-17082
DEBIAN	DSA-4353
REDHAT	RHSA-2019:2519
URL	https://bugs.php.net/bug.php?id=76582

Vulnerability Solution:

•Upgrade to PHP version 5.6.38

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

•Upgrade to PHP version 7.0.32

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

•Upgrade to PHP version 7.1.22

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

•Upgrade to PHP version 7.2.10

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

3.2.154. PHP Vulnerability: CVE-2018-5711 (php-cve-2018-5711)

Description:

gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1, has an integer signedness error that leads to an infinite loop via a crafted GIF file, as demonstrated by a call to the

imagecreatefromgif or imagecreatefromstring PHP function. This is related to GetCode_ and gdImageCreateFromGifCtx.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:80	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-2018-5711
REDHAT	RHSA-2018:1296
REDHAT	RHSA-2019:2519
URL	https://bugs.php.net/bug.php?id=75571

Vulnerability Solution:

•Upgrade to PHP version 5.6.33

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

•Upgrade to PHP version 7.0.27

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

•Upgrade to PHP version 7.1.13

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

•Upgrade to PHP version 7.2.1

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

3.2.155. 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:
10.0.2.4:80	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	5767

Vulnerability Solution:

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

3.2.156. Self-signed TLS/SSL certificate (ssl-self-signed-certificate)

Description:

The server's TLS/SSL certificate is self-signed. Self-signed certificates cannot be trusted by default, especially because TLS/SSL man-in-the-middle attacks typically use self-signed certificates to eavesdrop on TLS/SSL connections.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:25	TLS/SSL certificate is self-signed.
10.0.2.4:5432	TLS/SSL certificate is self-signed.

References:

None

Vulnerability Solution:

Obtain a new TLS/SSL server certificate that is NOT self-signed and install it on the server. The exact instructions for obtaining a new certificate depend on your organization's requirements. Generally, you will need to generate a certificate request and save the request as a file. This file is then sent to a Certificate Authority (CA) for processing. Your organization may have its own internal Certificate Authority. If not, you may have to pay for a certificate from a trusted external Certificate Authority, such as Thawte or Verisign.

3.2.157. TLS/SSL Server Supports SSLv3 (sslv3-supported)

Description:

The SSLv3 protocol and supported ciphers all suffer from serious vulnerabilities making this protocol unsafe to use.

The Payment Card Industry (PCI) Data Security Standard requires a minimum of TLS v1.1 and recommends TLS v1.2. In addition, FIPS 140-2 standard also requires a minimum of TLS v1.1 and recommends TLS v1.2.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
10.0.2.4:25	Successfully connected over SSLv3
10.0.2.4:5432	Successfully connected over SSLv3

References:

Source	Reference
CVE	CVE-2014-3566
URL	https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

Vulnerability Solution:

Configure the server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.

3.2.158. 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:
10.0.2.4:23	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.

3.2.159. TLS Server Supports TLS version 1.0 (tlsv1_0-enabled)

Description:

The PCI (Payment Card Industry) Data Security Standard requires a minimum of TLS v1.1 and recommends TLS v1.2. In addition, FIPS 140-2 standard requires a minimum of TLS v1.1 and recommends TLS v1.2.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:25	Successfully connected over TLSv1.0
10.0.2.4:5432	Successfully connected over TLSv1.0

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

Vulnerability Solution:

Configure the server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.

3.2.160. USN-1009-2: GNU C Library vulnerability (ubuntu-usn-1009-2)

Description:

USN-1009-1 fixed vulnerabilities in the GNU C library. Colin Watsondiscovered that the fixes were incomplete and introduced flaws withsetuid programs loading libraries that used dynamic string tokens in theirRPATH. If the "man" program was installed setuid, a local attacker couldexploit this to gain "man" user privileges, potentially leading to furtherprivilege 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libc6 2.7-10ubuntu5

References:

Source	Reference
USN	1009-2

Vulnerability Solution:

libc6 on Ubuntu Linux

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

3.2.161. 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:
10.0.2.4	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	12148
REDHAT	RHSA-2011:1749
REDHAT	RHSA-2013:0217
USN	1016-1

Vulnerability Solution:

libxml2 on Ubuntu Linux

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

3.2.162. 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:
10.0.2.4	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
OVAL	14638
OVAL	14804
REDHAT	RHSA-2011:0507
REDHAT	RHSA-2011:0844
REDHAT	RHSA-2011:0896
REDHAT	RHSA-2011:0897
USN	1134-1

Vulnerability Solution:

libapr1 on Ubuntu Linux

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

3.2.163. 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 wereable to perform a man-in-the-middle attack, this flaw could potentially beused to install altered packages. This update corrects the issue bydisabling the net-update option completely. A future update will re-enablethe 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu apt 0.7.9ubuntu17

References:

Source	Reference
USN	1215-1

Vulnerability Solution:

apt on Ubuntu Linux

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

3.2.164. USN-1427-1: MySQL vulnerabilities (ubuntu-usn-1427-1)

Description:

Multiple security issues were discovered in MySQL and this update includesnew upstream MySQL versions to fix these issues. MySQL has been updated to 5.1.62 in Ubuntu 10.04 LTS, Ubuntu 11.04 andUbuntu 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, newfeatures, and possibly incompatible changes. Please see the following for more information: http://dev.mysql.com/doc/refman/5.1/en/news-5-1-62.htmlhttp://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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu mysql-server-5.0 5.0.51a-3ubuntu5

References:

Source	Reference
USN	1427-1

Vulnerability Solution:

•mysql-server-5.0 on Ubuntu Linux

Upgrade mysql-server-5.0

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

•mysql-server-5.1 on Ubuntu Linux

Upgrade mysql-server-5.1

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

3.2.165. 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:
10.0.2.4	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	1461-1

Vulnerability Solution:

•postgresql-8.3 on Ubuntu Linux

Upgrade postgresql-8.3

Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version.

•postgresql-8.4 on Ubuntu Linux

Upgrade postgresql-8.4

Use `apt-get upgrade` to upgrade postgresql-8.4 to the latest version.

•postgresql-9.1 on Ubuntu Linux

Upgrade postgresql-9.1

Use `apt-get upgrade` to upgrade postgresql-9.1 to the latest version.

3.2.166. 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 usethis 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu gnupg 1.4.6-2ubuntu5

References:

Source	Reference
USN	1570-1

Vulnerability Solution:

•gnupg on Ubuntu Linux

Upgrade gnupg

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

•gnupg2 on Ubuntu Linux

Upgrade gnupg2

Use `apt-get upgrade` to upgrade gnupg2 to the latest version.

3.2.167. 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:
10.0.2.4	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	1686-1

Vulnerability Solution:

libfreetype6 on Ubuntu Linux

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

3.2.168. 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:
10.0.2.4	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	1752-1

Vulnerability Solution:

•libgnutls13 on Ubuntu Linux

Upgrade libgnutls13

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

•libgnutls26 on Ubuntu Linux

Upgrade libgnutls26

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

3.2.169. 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:
10.0.2.4	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	1782-1

Vulnerability Solution:
libxml2 on Ubuntu Linux
Use `apt-get upgrade` to upgrade libxml2 to the latest version.

3.2.170. 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:
10.0.2.4	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

Source	Reference
APPLE	APPLE-SA-2009-06-17-1
BID	30783
CVE	CVE-2008-3281
DEBIAN	DSA-1631
OVAL	6496
OVAL	9812
REDHAT	RHSA-2008:0836
USN	640-1

Vulnerability Solution:

libxml2 on Ubuntu Linux

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

3.2.171. 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 exploitthis to gain root privileges to the virtual machine by using apredictable password. This vulnerability only affects virtual machines created withvm-builder under Ubuntu 8.10, and does not affect native Ubuntuinstallations. An update was made to the shadow package to detectvulnerable systems and disable password authentication for theroot account. Vulnerable virtual machines which an attacker hasaccess to should be considered compromised, and appropriate actionstaken 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 thenecessary changes. https://bugs.launchpad.net/+bug/296841

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu passwd 1:4.0.18.2-1ubuntu2

References:

Source	Reference
USN	670-1

Vulnerability Solution:

•passwd on Ubuntu Linux

Upgrade passwd

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

•python-vm-builder on Ubuntu Linux

Upgrade python-vm-builder

Use `apt-get upgrade` to upgrade python-vm-builder to the latest version.

3.2.172. 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:
10.0.2.4	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	11650
REDHAT	RHSA-2008:0982
USN	678-1
XF	46482

Vulnerability Solution:

•libgnutls13 on Ubuntu Linux

Upgrade libgnutls13

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

•libgnutls26 on Ubuntu Linux

Upgrade libgnutls26

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

3.2.173. 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:
10.0.2.4	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	10874
OVAL	6252
REDHAT	RHSA-2009:1067
USN	753-1

Vulnerability Solution:
postgresql-8.3 on Ubuntu Linux
Use `apt-get upgrade` to upgrade postgresql-8.3 to the latest version.

3.2.174. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu libdbus-1-3 1.1.20-1ubuntu1

References:

Source	Reference
BID	31602
CVE	CVE-2009-1189
OVAL	10308
REDHAT	RHSA-2010:0095
USN	799-1
XF	50385

Vulnerability Solution:

libdbus-1-3 on Ubuntu Linux

Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version.

3.2.175. 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:
10.0.2.4	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	10414
OVAL	12245
OVAL	7806
USN	808-1

Vulnerability Solution:

bind9 on Ubuntu Linux

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

3.2.176. 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:
10.0.2.4	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	855-1
XF	53941

Vulnerability Solution:

libhtml-parser-perl on Ubuntu Linux

Use `apt-get upgrade` to upgrade libhtml-parser-perl to the latest version.

3.2.177. 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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu samba 3.0.20-0.1ubuntu1

References:

Source	Reference
CVE	CVE-2010-0926
USN	918-1

Vulnerability Solution:

samba on Ubuntu Linux

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

3.2.178. USN-928-1: Sudo vulnerability (ubuntu-usn-928-1)

Description:

Valerio Costamagna discovered that sudo did not properly validate the pathfor the 'sudoedit' pseudo-command when the PATH contained only a dot ('.').If secure_path and ignore_dot were disabled, a local attacker could exploitthis to execute arbitrary code as root if sudo was configured to allow theattacker to use sudoedit. By default, secure_path is used and the sudoeditpseudo-command is not used in Ubuntu. This is a different but related issueto 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 thenecessary changes. LP: 563963

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu sudo 1.6.9p10-1ubuntu3

References:

Source	Reference
USN	928-1

Vulnerability Solution:

•sudo on Ubuntu Linux

Upgrade sudo

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

•sudo-ldap on Ubuntu Linux

Upgrade sudo-ldap

Use `apt-get upgrade` to upgrade sudo-ldap to the latest version.

3.2.179. 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:
10.0.2.4	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

3.2.180. User umask value is unsafe (unix-umask-unsafe)

Description:

The umask value for the account used to scan this device 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:
10.0.2.4	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 via PAM. See 'man 8 pam_umask'. 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. For Red Hat Enterprise Linux and derivative distributions the umask value is set in /etc/profile and /etc/bashrc shell configuration files. See the Red Hat manual for more details.

3.2.181. 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:
10.0.2.4	The following world writable files were found./proc/1/attr/current (-rw-rw-rw-) /proc/1/attr/exec (-rw-rw-rw-)/proc/1/attr/fscreate (-rw-rw-rw-) /proc/1/attr/keycreate (-rw-rw-rw-)/proc/1/attr/sockcreate (-rw-rw-rw-) /proc/1/task/1/attr/current (-rw-rw-rw-)/proc/1/task/1/attr/exec (-rw-rw-rw-) /proc/1/task/1/attr/fscreate (-rw-rw-rw-)/proc/1/task/1/attr/keycreate (-rw-rw-rw-) /proc/1/task/1/attr/sockcreate (-rw-rw-rw-)/proc/1130/attr/current (-rw-rw-rw-) /proc/1130/attr/exec (-rw-rw-rw-)/proc/1130/attr/fscreate (-rw-rw-rw-) /proc/1130/attr/keycreate (-rw-rw-rw-)/proc/1130/attr/sockcreate (-rw-rw-rw-) /proc/1130/task/1130/attr/current (-rw-rw-rw-)/proc/1130/task/1130/attr/exec (-rw-rw-rw-)/proc/1130/task/1130/attr/fscreate (-rw-rw-rw-) /proc/1130/task/1130/attr/keycreate (-rw-rw-rw-) /proc/1130/task/1130/attr/sockcreate (-rw-rw-rw-)/proc/130/attr/current (-rw-rw-rw-)/proc/130/attr/exec (-rw-rw-rw-)/proc/130/attr/fscreate (-rw-rw-rw-) /proc/130/attr/keycreate (-rw-rw-rw-)/proc/130/attr/sockcreate (-rw-rw-rw-) /proc/130/task/130/attr/current (-rw-rw-rw-)/proc/130/task/130/attr/exec (-rw-rw-rw-)/proc/130/task/130/attr/fscreate (-rw-rw-rw-) /proc/130/task/130/attr/keycreate (-rw-rw-rw-)/proc/130/task/130/attr/sockcreate (-rw-rw-rw-)/proc/1301/attr/current (-rw-rw-rw-)/proc/1301/attr/exec (-rw-rw-rw-) /proc/1301/attr/fscreate (-rw-rw-rw-)/proc/1301/attr/keycreate (-rw-rw-rw-) /proc/1301/attr/sockcreate (-rw-rw-rw-)/proc/1301/task/1301/attr/current (-rw-rw-rw-)/proc/1301/task/1301/attr/exec (-rw-rw-rw-) /proc/1301/task/1301/attr/fscreate (-rw-rw-rw-) /proc/1301/task/1301/attr/keycreate (-rw-rw-rw-) /proc/1301/task/1301/attr/sockcreate (-rw-rw-rw-)/proc/1304/attr/current (-rw-rw-rw-)/proc/1304/attr/exec (-rw-rw-rw-)/proc/1304/attr/fscreate (-rw-rw-rw-) /proc/1304/attr/keycreate (-rw-rw-rw-)/proc/1304/attr/sockcreate (-rw-rw-rw-) /proc/1304/task/1304/attr/current (-rw-rw-rw-)/proc/1304/task/1304/attr/exec (-rw-rw-rw-)/proc/1304/task/1304/attr/fscreate (-rw-rw-rw-) /proc/1304/task/1304/attr/keycreate (-rw-rw-rw-) /proc/1304/task/1304/attr/sockcreate (-rw-rw-rw-)

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.

3.2.182. Unencrypted X11 Service Available (x11-open-port)

Description:

XWindows is an unencrypted protocol, as such it sends sensitive data in clear text.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:6000	Running XWindows service

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

Vulnerability Solution:
Stop the X Server from listening on TCP ports, ensure it is running with: -nolisten tcp
Replace it with other technologies like SSH with X-forwarding.

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:
10.0.2.4:80	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
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061101
IAVM	2015-A-0149
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: BIND 9 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:
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
10.0.2.4:53	Vulnerable OS: Ubuntu Linux 8.04 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
OVAL	10821
OVAL	11745
OVAL	7261
OVAL	7459
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:
10.0.2.4:3306	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
DEBIAN	DSA-2429
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. SHA-1-based Signature in TLS/SSL Server X.509 Certificate (tls-server-cert-sig-alg-sha1)

Description:

The SHA-1 hashing algorithm has known weaknesses that expose it to collision attacks, which may allow an attacker to generate additional X.509 digital certificates with the same signature as an original.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:25	SSL certificate is signed with SHA1withRSA
10.0.2.4:5432	SSL certificate is signed with SHA1withRSA

References:

Source	Reference
URL	https://technet.microsoft.com/en-us/library/security/2880823.aspx
URL	https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/
URL	http://googleonlinesecurity.blogspot.co.uk/2014/09/gradually-sunsetting-sha-1.html
URL	https://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html

Vulnerability Solution:

Stop using signature algorithms relying on SHA-1, such as "SHA1withRSA", when signing X.509 certificates. Instead, use the SHA-2 family (SHA-224, SHA-256, SHA-384, and SHA-512).

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:
10.0.2.4	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	1077-1

Vulnerability Solution:

fuse-utils on Ubuntu Linux

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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu apt 0.7.9ubuntu17

References:

Source	Reference

Source	Reference
CVE	CVE-2011-3634
USN	1283-1

Vulnerability Solution:

apt on Ubuntu Linux

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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu apt 0.7.9ubuntu17

References:

Source	Reference
BID	54046
CVE	CVE-2012-0954
USN	1477-1

Vulnerability Solution:

apt on Ubuntu Linux

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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu apache2.2-common 2.2.8-1ubuntu0.15

References:

Source	Reference
APPLE	APPLE-SA-2013-06-04-1
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
DEBIAN	DSA-3253
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061101
IAVM	2015-A-0149
OVAL	18832
OVAL	18920
OVAL	19539
REDHAT	RHSA-2012:1591
REDHAT	RHSA-2012:1592
REDHAT	RHSA-2012:1594
REDHAT	RHSA-2013:0130
REDHAT	RHSA-2013:0587
USN	1627-1

Vulnerability Solution:

apache2.2-common on Ubuntu Linux

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:
10.0.2.4	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: Ubuntu fuse-utils 2.7.2-1ubuntu2

References:

Source	Reference
BID	37983
CVE	CVE-2010-0789
DEBIAN	DSA-1989
USN	892-1
XF	55945

Vulnerability Solution:

fuse-utils on Ubuntu Linux

Use `apt-get upgrade` to upgrade fuse-utils to the latest version.

3.3.10. Weak Cryptographic Key (weak-crypto-key)

Description:

The key length used by a cryptographic algorithm determines the highest security it can offer. Newly discovered theoretical attacks and hardware advances constantly erode this security level over time. Taking this into account, as of 2011, governmental, academic, and private organizations providing guidance on cryptographic security, such as the National Institute of Standards and Technology (NIST), the European Network of Excellence in Cryptology II (ECRYPT II), make the following general recommendations to provide short to medium term security against even the most well-funded attackers (eg. intelligence agencies):

•Symmetric key lengths of at least 80-112 bits.

•Elliptic curve key lengths of at least 160-224 bits.

•RSA key lengths of at least 1248-2048 bits. In particular, the CA/Browser Forum Extended Validation (EV) Guidelines require a minimum key length of 2048 bits. Also, current research shows that factoring a 1024-bit RSA modulus is within practical reach.

•DSA key lengths of at least 2048 bits.

Additionally, starting in 2014, the Certificate Authority/Browser Forum has mandated that 1024-bit RSA keys no longer be supported for SSL certificates or code signing.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4:25	Length of RSA modulus in X.509 certificate: 1024 bits (less than 2047 bits)
10.0.2.4:5432	Length of RSA modulus in X.509 certificate: 1024 bits (less than 2047 bits)

References:

Source	Reference
URL	http://csrc.nist.gov/groups/ST/toolkit/key_management.html
URL	http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf
URL	http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2011_2_AlgoKatpdf.pdf
URL	http://www.ecrypt.eu.org/documents/D.SPA.17.pdf
URL	http://www.keylength.com
URL	http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf
URL	http://www.symantec.com/page.jsp?id=1024-bit-certificate-support

Vulnerability Solution:

If the weak key is used in an X.509 certificate (for example for an HTTPS server), generate a longer key and recreate the certificate. Please also refer to NIST's recommendations on cryptographic algorithms and key lengths.

3.3.11. 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:
10.0.2.4:3306	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

Source	Reference
DEBIAN	DSA-2429
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.

3.3.12. 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:
10.0.2.4:80	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
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

3.3.13. 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:
10.0.2.4:25	Running SMTP serviceProduct Postfix exists -- Postfix 2.5.1Vulnerable 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.

3.3.14. 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:
10.0.2.4	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	1044-1

Vulnerability Solution:

libdbus-1-3 on Ubuntu Linux

Use `apt-get upgrade` to upgrade libdbus-1-3 to the latest version.

3.3.15. 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:
10.0.2.4	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	642-1
XF	44865

Vulnerability Solution:

postfix on Ubuntu Linux
Use `apt-get upgrade` to upgrade postfix to the latest version.

3.3.16. 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:
10.0.2.4	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.

3.3.17. User home directory mode unsafe (unix-user-home-dir-mode)

Description:

A user's home directory was found to have permission mode above 750 (Owner=READ/WRITE/EXECUTE, Group=READ/EXECUTE, Other=NONE). "Group" or "Other" WRITE permissions means that a malicious user may gain complete access to user data by escalating privileges. In addition "read" and "execute" access for "Other" should always be disabled (sensitive data access).

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4	The permissions for home directory of user msfadmin was found to be 755 instead of 750.
10.0.2.4	The permissions for home directory of user service was found to be 755 instead of 750.
10.0.2.4	The permissions for home directory of user user 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

3.3.18. CIFS Share Readable By Guest (cifs-share-world-readable)

Description:

A share was found which allows read access by the guest account or anonymously. The impact of this vulnerability depends on the contents of the share.

Affected Nodes:

Affected Nodes:	Additional Information:
10.0.2.4	Sucessfully read share "tmp" and found the following files: #sql1083_208_0.MYD.ICE-unix#sql1083_208_0.MYIorbit-msfadmin.X11-unix .X0-lock#sql1083_208_0.frm4584.jsvc_upgconfd-msfadmin

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.

3.3.19. 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 target's 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:
10.0.2.4:53	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.

3.3.20. 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:
10.0.2.4:21	Running FTP serviceSuccessfully 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.

3.3.21. 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:

Affected Nodes:	Additional Information:
10.0.2.4:21	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.

3.3.22. 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:
10.0.2.4	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).

3.3.23. 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:
10.0.2.4	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.

3.3.24. 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:
10.0.2.4:137	Running CIFS Name Service serviceConfiguration item advertised-name-count set to '7' 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.

3.3.25. 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:
10.0.2.4:22	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.

3.3.26. 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:
10.0.2.4	Received UDP packet with IP ID of zero:IPv4 SRC[10.0.2.4] TGT[10.0.2.15] TOS[0] TTL[64] Flags[40] Proto[17] ID[0] FragOff[0] HDR-LENGTH[20] TOTAL-LENGTH[52] CKSUM[8871] UDP SRC-PORT[2049] TGT-PORT[37282] CKSUM[11071] RAW DATA [24]: 3EECE3CA00000001000000000000000 >..... 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. CIFS

CIFS, the Common Internet File System, was defined by Microsoft to provide file sharing services over the Internet. CIFS extends the Server Message Block (SMB) protocol designed by IBM and enhanced by Intel and Microsoft. CIFS provides mechanisms for sharing resources (files, printers, etc.) and executing remote procedure calls over named pipes.

4.1.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	139	4	•Samba 3.0.20-Debian •domain: METASPLOITABLE •password-mode: encrypt •security-mode: user •smb-signing: disabled •smb1-enabled: true
10.0.2.4	tcp	445	4	•Samba 3.0.20-Debian •domain: METASPLOITABLE •password-mode: encrypt •security-mode: user •smb-signing: disabled •smb1-enabled: true

4.2. CIFS Name Service

CIFS, the Common Internet File System, was defined by Microsoft to provide file sharing services over the Internet. CIFS extends the Server Message Block (SMB) protocol designed by IBM and enhanced by Intel and Microsoft. CIFS provides mechanisms for sharing resources (files, printers, etc.) and executing remote procedure calls over named pipes. This service is used to handle CIFS browsing (name) requests. Responses contain the names and types of services that can be accessed via CIFS named pipes.

4.2.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	udp	137	1	•advertised-name-1: METASPLOITABLE (Computer Name) •advertised-name-2: METASPLOITABLE (Logged-on User) •advertised-name-3: METASPLOITABLE (File Server Service) •advertised-name-4: __MSBROWSE__ (Master Browser)

Device	Protocol	Port	Vulnerabilities	Additional Information
				•advertised-name-5: WORKGROUP (Domain Name) •advertised-name-6: WORKGROUP (Master Browser) •advertised-name-7: WORKGROUP (Browser Service Elections) •advertised-name-count: 7 •mac-address: 000000000000

4.3. DNS

DNS, the Domain Name System, provides naming services on the Internet. DNS is primarily used to convert names, such as www.rapid7.com to their corresponding IP address for use by network programs, such as a browser.

4.3.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	53	0	•BIND 9.4.2 •bind.version: 9.4.2
10.0.2.4	udp	53	1	•BIND 9.4.2 •bind.version: 9.4.2
10.0.2.4	tcp	53	1	
10.0.2.4	udp	53	1	
10.0.2.4	tcp	53	1	
10.0.2.4	udp	53	1	
10.0.2.4	tcp	53	1	
10.0.2.4	udp	53	1	
10.0.2.4	tcp	53	1	
10.0.2.4	udp	53	1	
10.0.2.4	tcp	53	1	
10.0.2.4	udp	53	1	
10.0.2.4	tcp	53	1	
10.0.2.4	udp	53	1	
10.0.2.4	tcp	53	1	
10.0.2.4	udp	53	1	

4.4. FTP

FTP, the File Transfer Protocol, is used to transfer files between systems. On the Internet, it is often used on web pages to download files from a web site using a browser. FTP uses two connections, one for control connections used to authenticate, navigate the FTP

server and initiate file transfers. The other connection is used to transfer data, such as files or directory listings.

4.4.1. General Security Issues

Cleartext authentication

The original FTP specification only provided means for authentication with cleartext user ids and passwords. Though FTP has added support for more secure mechanisms such as Kerberos, cleartext authentication is still the primary mechanism. If a malicious user is in a position to monitor FTP traffic, user ids and passwords can be stolen.

4.4.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	21	2	•vsFTPd 2.3.4 •ftp.banner: 220 (vsFTPd 2.3.4) •ftp.plaintext.authentication: true

4.5. HTTP

HTTP, the HyperText Transfer Protocol, is used to exchange multimedia content on the World Wide Web. The multimedia files commonly used with HTTP include text, sound, images and video.

4.5.1. General Security Issues

Simple authentication scheme

Many HTTP servers use BASIC as their primary mechanism for user authentication. This is a very simple scheme that uses base 64 to encode the cleartext user id and password. If a malicious user is in a position to monitor HTTP traffic, user ids and passwords can be stolen by decoding the base 64 authentication data. To secure the authentication process, use HTTPS (HTTP over TLS/SSL) connections to transmit the authentication data.

4.5.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	80	9	•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
10.0.2.4	tcp	8180	3	•Apache Tomcat •Coyote: 1.1 •http.banner: Apache-Coyote/1.1

Device	Protocol	Port	Vulnerabilities	Additional Information
				•http.banner.server: Apache-Coyote/1.1

4.6. MySQL

4.6.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	3306	8	•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 •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

Device	Protocol	Port	Vulnerabilities	Additional Information
				•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 •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_awe_mem_mb: 0

Device	Protocol	Port	Vulnerabilities	Additional Information
				•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 •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/

Device	Protocol	Port	Vulnerabilities	Additional Information
				•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 •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

Device	Protocol	Port	Vulnerabilities	Additional Information
				•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 •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

Device	Protocol	Port	Vulnerabilities	Additional Information
				•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 •service.banner: 5.0.51a-3ubuntu5 •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 •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: EST •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

Device	Protocol	Port	Vulnerabilities	Additional Information
				•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

4.7. NFS

The Network File System provides remote file access to shared file systems across a network. NFS provides methods to list and browse directories and to access and alter files. NFS is built on the RPC protocol and is thus independent of machine, operating systems, or even underlying protocol. The main NFS protocol often operates in tandem with other NFS style protocols. The NFS Mount protocol deals with attaching the remote file systems to a point on the local machine's file system, and advertising what file systems are available to be mounted. The NFS Lock manager adds support for file locking to prevent the occurrence of file change conflicts.

4.7.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	2049	0	•program-number: 100003 •program-version: 4
10.0.2.4	udp	2049	0	•program-number: 100003 •program-version: 4

4.8. NFS lockd

The Network File System provides remote file access to shared file systems across a network. NFS provides methods to list and browse directories and to access and alter files. NFS is built on the RPC protocol and is thus independent of machine, operating systems, or even underlying protocol. This service, NFS Lock manager, adds support for file locking to prevent the occurrence of file change conflicts. Since the NFS protocol is stateless, the NFS Lock Manager takes care of all the stateful aspects of file locking across a network

4.8.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	42095	0	•program-number: 100021 •program-version: 4
10.0.2.4	udp	60553	0	•program-number: 100021 •program-version: 4

4.9. Postgres

4.9.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	5432	5	•ssl.cert.chainerror: [Path does not chain with any of the trust anchors] •ssl.cert.issuer.dn: EMAILADDRESS=root@ubuntu804-base.localdomain, CN=ubuntu804-base.localdomain, OU=Office for Complication of Otherwise Simple Affairs, O=OCOSA, L=Everywhere, ST=There is no such thing outside US, C=XX •ssl.cert.key.alg.name: RSA •ssl.cert.key.rsa.modulusBits: 1024 •ssl.cert.not.valid.after: Fri, 16 Apr 2010 10:07:45 EDT •ssl.cert.not.valid.before: Wed, 17 Mar 2010 10:07:45 EDT •ssl.cert.selfsigned: true •ssl.cert.serial.number: 18084549878917544396 •ssl.cert.sha1.fingerprint: ed093088706603bfd5dc237399b498da2d4d31c6 •ssl.cert.sig.alg.name: SHA1withRSA •ssl.cert.subject.dn: EMAILADDRESS=root@ubuntu804-base.localdomain, CN=ubuntu804-base.localdomain, OU=Office for Complication of Otherwise Simple Affairs, O=OCOSA, L=Everywhere, ST=There is no such thing outside US, C=XX •ssl.cert.validchain: false •ssl.cert.validsignature: true •ssl.cert.version: 1 •ssl.dh.generator.1024: 2 •ssl.dh.prime.1024:

Device	Protocol	Port	Vulnerabilities	Additional Information
				f488fd584e49dbcd20b49de49107366b 336c380d451d0f7c88b31c7c5b2d8ef6 f3c923c043f0a55b188d8ebb558cb85d 38d334fd7c175743a31d186cde33212 cb52aff3ce1b1294018118d7c84a70a7 2d686c40319c807297aca950cd9969f abd00a509b0246d3083d66a45d419f9 c7cbd894b221926baaba25ec355e92f 78c7 •ssl.protocols: sslv3,tlsv1_0 •sslv3: true •sslv3.TLS_DHE_RSA_WITH_3DES_E DE_CBC_SHA.dh.keysize: 1024 •sslv3.TLS_DHE_RSA_WITH_AES_12 8_CBC_SHA.dh.keysize: 1024 •sslv3.TLS_DHE_RSA_WITH_AES_25 6_CBC_SHA.dh.keysize: 1024 •sslv3.ciphers: TLS_RSA_WITH_3DES_EDE_CBC_ SHA,TLS_RSA_WITH_RC4_128_SH A,TLS_DHE_RSA_WITH_3DES_EDE _CBC_SHA,TLS_RSA_WITH_AES_2 56_CBC_SHA,TLS_RSA_WITH_AES _128_CBC_SHA,TLS_DHE_RSA_WI TH_AES_256_CBC_SHA,TLS_DHE_ RSA_WITH_AES_128_CBC_SHA •sslv3.extensions: RENEGOTIATION_INFO •starttls-protocol: Postgres •supports-starttls: true •tlsv1_0: true •tlsv1_0.TLS_DHE_RSA_WITH_3DES _EDE_CBC_SHA.dh.keysize: 1024 •tlsv1_0.TLS_DHE_RSA_WITH_AES_ 128_CBC_SHA.dh.keysize: 1024 •tlsv1_0.TLS_DHE_RSA_WITH_AES_ 256_CBC_SHA.dh.keysize: 1024 •tlsv1_0.ciphers: TLS_RSA_WITH_3DES_EDE_CBC_ SHA,TLS_RSA_WITH_RC4_128_SH

Device	Protocol	Port	Vulnerabilities	Additional Information
				A,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA •tlsv1_0.extensions: RENEGOTIATION_INFO •tlsv1_1: false •tlsv1_2: false

4.10. Remote Execution

Remote Execution, rexec, is used to execute a command on a remote system.

4.10.1. General Security Issues

Authentication easily spoofed

The Remote Execution protocol does not use userid/password authentication to validate users. Instead it uses trust relationships based on information that is easily spoofed by an attacker. When a client connects to a rexec server, it sends a user name to the server. The server verifies client access by: 1. verifying the client's TCP port is reserved (below 1024) 2. verifying that the specified user name exists 3. verifying the client's IP address is in /etc/hosts.equiv file (or /.rhosts if root was specified as the user name). 4. verifying that logins have not been disabled (eg, /etc/nologin).

4.10.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	512	1	

4.11. Remote Login

Remote Login, rlogin, is used to create a virtual terminal on the remote system, similar to a Telnet connection. Unlike Telnet connections, rlogin does not require a password from trusted hosts.

4.11.1. General Security Issues

Authentication easily spoofed

The Remote Login protocol does not use userid/password authentication to validate users. Instead it uses trust relationships based on information that is easily spoofed by an attacker. When a client connects to a rlogin server, it sends a user name to the server. The server verifies client access by: 1. verifying the client's TCP port is reserved (below 1024) 2. verifying that the specified user name exists 3. verifying the client's IP address is in /etc/hosts.equiv file (or /.rhosts if root was specified as the user name). 4. verifying that logins have not been disabled (eg, /etc/nologin).

4.11.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	513	1	

4.12. Remote Shell

Remote Shell, rsh, is used to open a shell on the remote system. Once a shell is established, the client can execute commands on the remote system and receive the program output.

4.12.1. General Security Issues

Authentication easily spoofed

The Remote Shell protocol does not use userid/password authentication to validate users. Instead it uses trust relationships based on information that is easily spoofed by an attacker. When a client connects to a rsh server, it sends a user name to the server. The server verifies client access by: 1. verifying the client's TCP port is reserved (below 1024) 2. verifying that the specified user name exists 3. verifying the client's IP address is in /etc/hosts.equiv file (or /.rhosts if root was specified as the user name). 4. verifying that logins have not been disabled (eg, /etc/nologin).

4.12.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	514	1	

4.13. SMTP

SMTP, the Simple Mail Transfer Protocol, is the Internet standard way to send e-mail messages between hosts. Clients typically submit outgoing e-mail to their SMTP server, which then forwards the message on through other SMTP servers until it reaches its final destination.

4.13.1. General Security Issues

Installed by default

By default, most UNIX workstations come installed with the sendmail (or equivalent) SMTP server to handle mail for the local host (e.g. the output of some cron jobs is sent to the root account via email). Check your workstations to see if sendmail is running, by telnetting to port 25/tcp. If sendmail is running, you will see something like this: $ telnet mybox 25 Trying 192.168.0.1... Connected to mybox. Escape character is '^]'. 220 mybox. ESMTP Sendmail 8.12.2/8.12.2; Thu, 9 May 2002 03:16:26 -0700 (PDT) If sendmail is running and you don't need it, then disable it via /etc/rc.conf or your operating system's equivalent startup configuration file. If you do need SMTP for the localhost, make sure that the server is only listening on the loopback interface (127.0.0.1) and is not reachable by other hosts. Also be sure to check port 587/tcp, which some versions of sendmail use for outgoing mail submissions.

Promiscuous relay

Perhaps the most common security issue with SMTP servers is servers which act as a "promiscuous relay", or "open relay". This describes servers which accept and relay mail from anywhere to anywhere. This setup allows unauthenticated 3rd parties (spammers) to use your mail server to send their spam to unwitting recipients. Promiscuous relay checks are performed on all discovered SMTP servers. See "smtp-general-openrelay" for more information on this vulnerability and how to fix it.

4.13.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	25	6	•Postfix •Postfix 2.5.1 •advertise-esmtp: 1 •advertised-esmtp-extension-count: 8 •advertises-esmtp: true •max-message-size: 10240000 •smtp.banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu) •smtp.plaintext.authentication: false •ssl.cert.chainerror: [Path does not chain with any of the trust anchors] •ssl.cert.issuer.dn: EMAILADDRESS=root@ubuntu804-base.localdomain, CN=ubuntu804-base.localdomain, OU=Office for Complication of Otherwise Simple Affairs, O=OCOSA, L=Everywhere, ST=There is no such thing outside US, C=XX •ssl.cert.key.alg.name: RSA •ssl.cert.key.rsa.modulusBits: 1024 •ssl.cert.not.valid.after: Fri, 16 Apr 2010 10:07:45 EDT •ssl.cert.not.valid.before: Wed, 17 Mar 2010 10:07:45 EDT •ssl.cert.selfsigned: true •ssl.cert.serial.number: 18084549878917544396 •ssl.cert.sha1.fingerprint: ed093088706603bfd5dc237399b498da2d4d31c6 •ssl.cert.sig.alg.name: SHA1withRSA •ssl.cert.subject.dn: EMAILADDRESS=root@ubuntu804-base.localdomain, CN=ubuntu804-base.localdomain, OU=Office for Complication of Otherwise Simple Affairs, O=OCOSA, L=Everywhere, ST=There is no such thing outside US,

Device	Protocol	Port	Vulnerabilities	Additional Information
				C=XX •ssl.cert.validchain: false •ssl.cert.validsignature: true •ssl.cert.version: 1 •ssl.dh.generator.1024: 2 •ssl.dh.generator.512: 2 •ssl.dh.prime.1024: b0feb4cfd45507e7cc88590d1726c50ca54a92238178da88aa4c1306bf5d2f9ebc96b851009d0c0d75adfd3bb17e714f3f91541444b830251cebdf729c4cf1890d683f948ea4fb768918b29116900199668c53814e273d99e75a7aafd5ece27efaed0118c2782559065c39f6cd4954afc1b1ea4af953d0df6dafd493e7baae9b •ssl.dh.prime.512: 883f00affc0c8ab835cde5c20f55df063f1607bfce1335e41c1e03f3ab17f6635063673e10d73eb4eb468c4050e691a56e0145dec9b11f6454fad9ab4f70ba5b •ssl.protocols: sslv3,tlsv1_0 •sslv3: true •sslv3.TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA.dh.keysize: 512 •sslv3.TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.dh.keysize: 1024 •sslv3.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 1024 •sslv3.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 1024 •sslv3.ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_EXPORT_WITH_DES40_CBC_SHA,TLS_DH_anon_WITH_DES_CBC_SHA,TLS_RSA_WITH_RC4_128_MD5,TLS_DH_anon_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,T

Device	Protocol	Port	Vulnerabilities	Additional Information
				LS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_DES_CBC_SHA,TLS_DH_anon_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5,TLS_RSA_EXPORT_WITH_RC4_40_MD5,TLS_DHE_RSA_WITH_DES_CBC_SHA,TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA,TLS_DH_anon_EXPORT_WITH_RC4_40_MD5,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_DH_anon_WITH_RC4_128_MD5,TLS_DH_anon_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA •sslv3.extensions: RENEGOTIATION_INFO •starttls-protocol: SMTP •supports-8bitmime: true •supports-debug: FALSE •supports-dsn: true •supports-enhancedstatuscodes: true •supports-etrn: true •supports-expand: FALSE •supports-pipelining: true •supports-size: true •supports-starttls: true •supports-turn: FALSE •supports-verify: FALSE •supports-vrfy: true •tlsv1_0: true •tlsv1_0.TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA.dh.keysize: 512 •tlsv1_0.TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.dh.keysize: 1024 •tlsv1_0.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 1024

Device	Protocol	Port	Vulnerabilities	Additional Information
				•tlsv1_0.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 1024 •tlsv1_0.ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_EXPORT_WITH_DES40_CBC_SHA,TLS_DH_anon_WITH_DES_CBC_SHA,TLS_RSA_WITH_RC4_128_MD5,TLS_DH_anon_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_DES_CBC_SHA,TLS_DH_anon_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5,TLS_RSA_EXPORT_WITH_RC4_40_MD5,TLS_DHE_RSA_WITH_DES_CBC_SHA,TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA,TLS_DH_anon_EXPORT_WITH_RC4_40_MD5,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_DH_anon_WITH_RC4_128_MD5,TLS_DH_anon_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA •tlsv1_0.extensions: RENEGOTIATION_INFO •tlsv1_1: false •tlsv1_2: false

4.14. SSH

SSH, or Secure SHell, is designed to be a replacement for the aging Telnet protocol. It primarily adds encryption and data integrity to Telnet, but can also provide superior authentication mechanisms such as public key authentication.

4.14.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	22	2	•OpenBSD OpenSSH 4.7p1

Device	Protocol	Port	Vulnerabilities	Additional Information
				•ssh.banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 •ssh.protocol.version: 2.0 •ssh.rsa.pubkey.fingerprint: 5656240F211DDEA72BAE61B1243D E8F3

4.15. Shell Backdoor

4.15.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	1524	1	•system: unix •unix.shell: bash

4.16. Telnet

The telnet service provides console access to a machine remotely. All data, including usernames and passwords, is sent in cleartext over TCP. In recent times, most networks have phased out its use in favor for the SSH, or Secure SHell, protocol, which primarily provides strong encryption and superior authentication mechanisms.

4.16.1. General Security Issues

No Support For Encryption

The number one vulnerability that the telnet service faces is its inherent lack of support for encryption. This is an artifact from the time period in which it was invented, 1971. There existed little knowledge of cryptography outside of military environments, and computer technology was not yet advanced enough to handle its real-time use. SSH should be used instead of telnet.

System Architecture Information Leakage

Most telnet servers will broadcast a banner which details the exact system type (ie: hardware and operating system versions) to any connecting client, without requiring authentication. This information is crucial for carrying out serious attacks on the system.

4.16.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	23	1	•telnet.banner: _ _ _ _ _ _ _ _____ _ __ ____ ____| |_ ___ _ ____ _ __ | | ___ (_) |_ __ _| |__ | | ____|____ \ | '_ ` _ \ / _ \ __/ _` / __| '_ \ |/ _ \ | | __/ _` | '_ \ |/ _ \ __) | | | | | | __/ || (_| \ __ \ |_) | | (_) | | || (_| | |_) | | __// __/ |_| |_| |_|____|__|__,_|____/ .__/|_|____/|_|__|__,_|_.__/|_|____|___

Device	Protocol	Port	Vulnerabilities	Additional Information
				__| |_| Warning: Never expose this VM to an untrusted network! Contact: msfdev[at]metasploit.com Login with msfadmin/msfadmin to get started metasploitable login:

4.17. VNC

AT&T VNC is used to provide graphical control of a system. A VNC server can run on a Microsoft Windows, Apple Macintosh or Unix (X Windows) system. By supplying the appropriate password, a VNC server system can be accessed by a VNC client. Full control of the system is provided through VNC, including command execution.

4.17.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	5900	2	•protocol-version: 3.3 •supported-auth-1: VNC Authentication •supported-auth-count: 1

4.18. XWindows

4.18.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	6000	1	

4.19. mountd

4.19.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	40935	1	•program-number: 100005 •program-version: 3
10.0.2.4	udp	54020	1	•program-number: 100005 •program-version: 3

4.20. portmapper

The Remote Procedure Call portmapper is a service that maps RPC programs to specific ports, and provides that information to client programs. Since most RPC programs do not have a well defined port number, they are dynamically allocated a port number when they are first run. Any client program that wishes to use a particular RPC program first contacts the portmapper to determine the port and protocol of the specified RPC program. The client then uses that information to contact the RPC program directly. In addition some implementations of the portmapper allow tunneling commands to RPC programs through the portmapper.

4.20.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	111	0	•program-number: 100000 •program-version: 2
10.0.2.4	udp	111	0	•program-number: 100000 •program-version: 2

4.21. status

4.21.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.0.2.4	tcp	55526	0	•program-number: 100024 •program-version: 1
10.0.2.4	udp	59163	0	•program-number: 100024 •program-version: 1

5. Discovered Users and Groups

5.1. System

5.1.1. 10.0.2.4

Account Name	Type	Additional Information
AnonymousLogon	Group	•comment: AnonymousLogon •group-id: 7
Authenticated Users	Group	•comment: Authenticated Users •group-id: 11
Batch	Group	•comment: Batch •group-id: 3
Creator Group	Group	•comment: Creator Group •group-id: 1
Creator Owner	Group	•comment: Creator Owner
Dialup	Group	•comment: Dialup •group-id: 1
Everyone	Group	•comment: Everyone
Interactive	Group	•comment: Interactive •group-id: 4
Local Service	Group	•comment: Local Service •group-id: 19
Network	Group	•comment: Network •group-id: 2
Network Service	Group	•comment: Network Service •group-id: 20
Proxy	Group	•comment: Proxy •group-id: 8
Remote Interactive Logon	Group	•comment: Remote Interactive Logon •group-id: 14
Restricted	Group	•comment: Restricted •group-id: 12
SYSTEM	Group	•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	User	•comment: •user-id: 1068
bin	User	•comment: •user-id: 1004
bind	Group	•group-id: 113
cdrom	Group	•group-id: 24
crontab	Group	•group-id: 108
daemon	User	•gid: 1 •loginShell: /bin/sh •password: x •user-id: 1 •userDir: /usr/sbin
dhcp	User	•gid: 102 •loginShell: /bin/false •password: x •user-id: 101 •userDir: /nonexistent
dialout	Group	•group-id: 20
dip	Group	•group-id: 30

Account Name	Type	Additional Information
disk	Group	•group-id: 6
distccd	User	•comment: •user-id: 1222
fax	Group	•group-id: 21
floppy	Group	•group-id: 25
ftp	User	•comment: •user-id: 1214
fuse	Group	•group-id: 107
games	Group	•group-id: 60
gnats	User	•comment: •full-name: Gnats Bug-Reporting System (admin) •user-id: 1082
irc	Group	•group-id: 39
klog	User	•comment: •user-id: 1206
kmem	Group	•group-id: 15
libuuid	User	•gid: 101 •loginShell: /bin/sh •password: x •user-id: 100 •userDir: /var/lib/libuuid
list	Group	•group-id: 38
lp	User	•gid: 7 •loginShell: /bin/sh •password: x •user-id: 7 •userDir: /var/spool/lpd
lpadmin	Group	•group-id: 111
mail	User	•gid: 8 •loginShell: /bin/sh •password: x •user-id: 8 •userDir: /var/mail
man	User	•comment:

Account Name	Type	Additional Information
		•user-id: 1012
mlocate	Group	•group-id: 109
msfadmin	User	•full-name: msfadmin,,, •gid: 1000 •loginShell: /bin/bash •password: x •user-id: 1000 •userDir: /home/msfadmin
mysql	User	•full-name: MySQL Server,,, •gid: 118 •loginShell: /bin/false •password: x •user-id: 109 •userDir: /var/lib/mysql
news	User	•comment: •user-id: 1018
nobody	User	•gid: 65534 •loginShell: /bin/sh •password: x •user-id: 65534 •userDir: /nonexistent
nogroup	Group	•group-id: 65534
nvram	Group	•group-id: 106
operator	Group	•group-id: 37
plugdev	Group	•group-id: 46
postdrop	Group	•group-id: 116
postfix	User	•gid: 115 •loginShell: /bin/false •password: x •user-id: 106 •userDir: /var/spool/postfix
postgres	User	•comment: •full-name: PostgreSQL administrator,,, •user-id: 1216
proftpd	User	•gid: 65534

Account Name	Type	Additional Information
		•loginShell: /bin/false •password: x •user-id: 113 •userDir: /var/run/proftpd
proxy	User	•gid: 13 •loginShell: /bin/sh •password: x •user-id: 13 •userDir: /bin
root	Group	
sambashare	Group	•group-id: 119
sasl	Group	•group-id: 45
scanner	Group	•group-id: 105
service	User	•comment: •full-name: ,,, •user-id: 3004
shadow	Group	•group-id: 42
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 •loginShell: /bin/false •password: x •user-id: 114 •userDir: /var/lib/nfs
sudo	Group	•group-id: 27
sync	User	•gid: 65534 •loginShell: /bin/sync

Account Name	Type	Additional Information
		•password: x •user-id: 4 •userDir: /bin
sys	User	•gid: 3 •loginShell: /bin/sh •password: x •user-id: 3 •userDir: /dev
syslog	User	•gid: 103 •loginShell: /bin/false •password: x •user-id: 102 •userDir: /home/syslog
tape	Group	•group-id: 26
telnetd	User	•comment: •user-id: 1224
tomcat55	User	•gid: 65534 •loginShell: /bin/false •password: x •user-id: 110 •userDir: /usr/share/tomcat5.5
tty	Group	•group-id: 5
user	Group	•group-id: 1001
users	Group	•group-id: 100
utmp	Group	•group-id: 43
uucp	User	•comment: •user-id: 1020
video	Group	•group-id: 44
voice	Group	•group-id: 22
www-data	User	•comment: •user-id: 1066

5.2. MySQL

5.2.1. 10.0.2.4

Account Name	Type	Additional Information
debian-sys-maint	User	
guest	User	
root	User	

6. Discovered Databases

6.1. MySQL

6.1.1. 10.0.2.4

•dvwa
•information_schema
•metasploit
•mysql
•owasp10
•tikiwiki
•tikiwiki195

7. Discovered Files and Directories

7.1. 10.0.2.4

File/Directory Name	Type	Properties
opt	Directory	•comment: •mount-point: C:\tmp
print$	Directory	•comment: Printer Drivers •mount-point: C:\var\lib\samba\printers
tmp	Directory	•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.