Audit Report

Tests

Audited on April 16, 2018

Reported on April 16, 2018

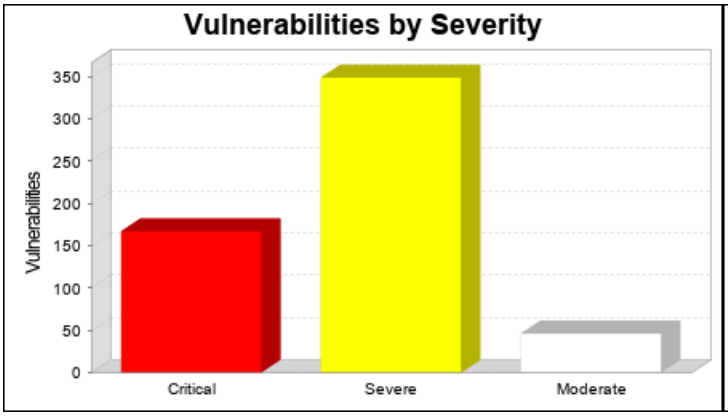
1. Executive Summary

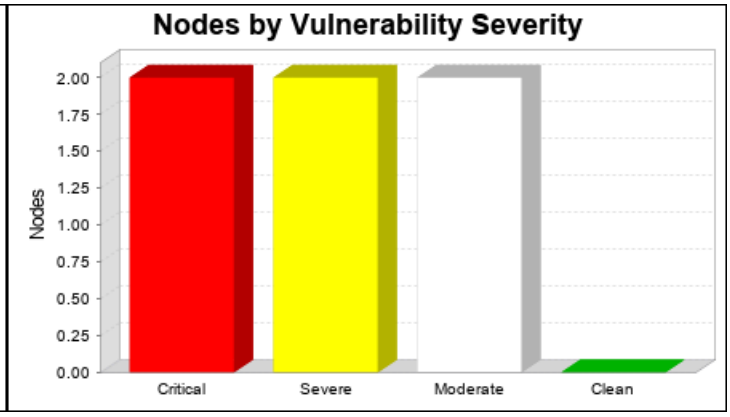
This report represents a security audit performed by Nexpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
Test	April 16, 2018 17:26, EEST	April 16, 2018 17:48, EEST	22 minutes	Success

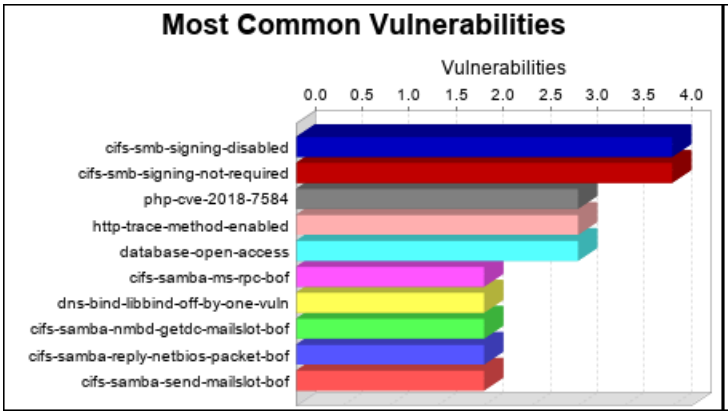
There is not enough historical data to display risk trend.

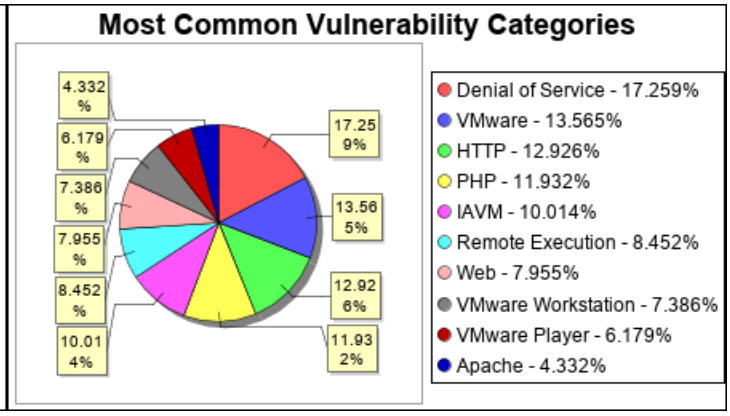
The audit was performed on 2 systems, 2 of which were found to be active and were scanned.



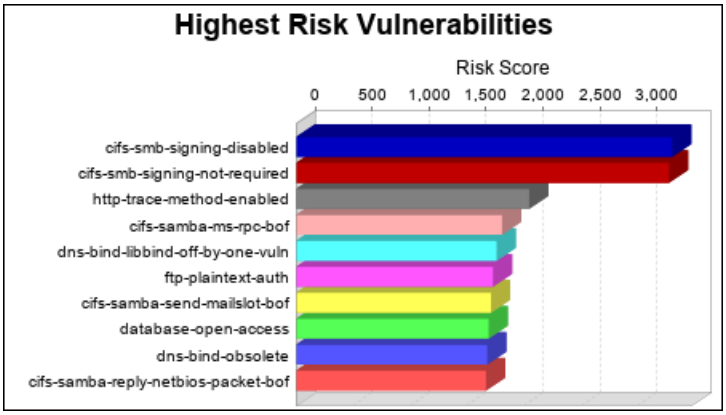


There were 562 vulnerabilities found during this scan. Of these, 167 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 349 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 46 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. Critical vulnerabilities were found to exist on 2 of the systems, making them most susceptible to attack. 2 systems were found to have severe vulnerabilities. Moderate vulnerabilities were found on 2 systems. No systems were free of vulnerabilities.

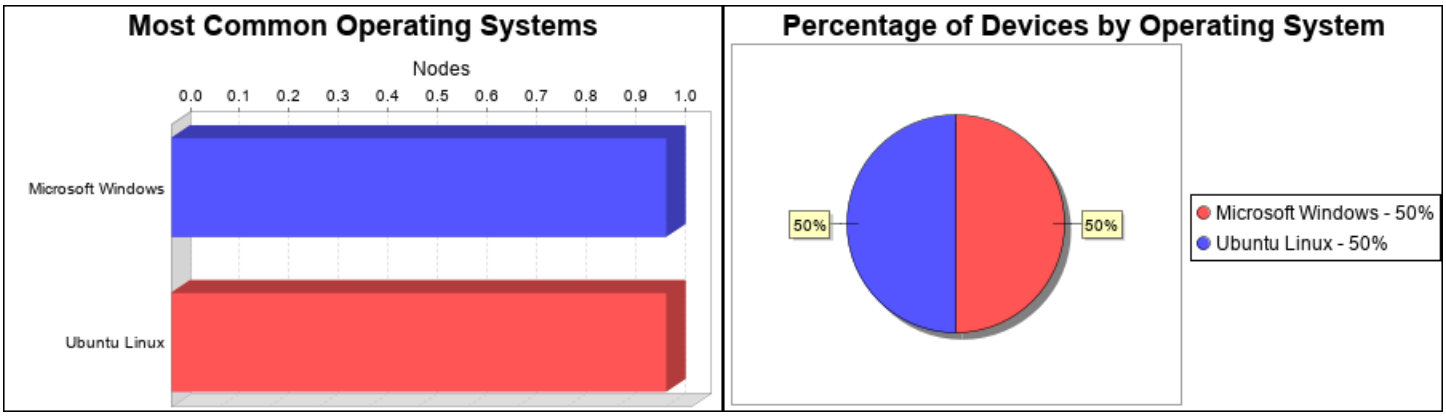




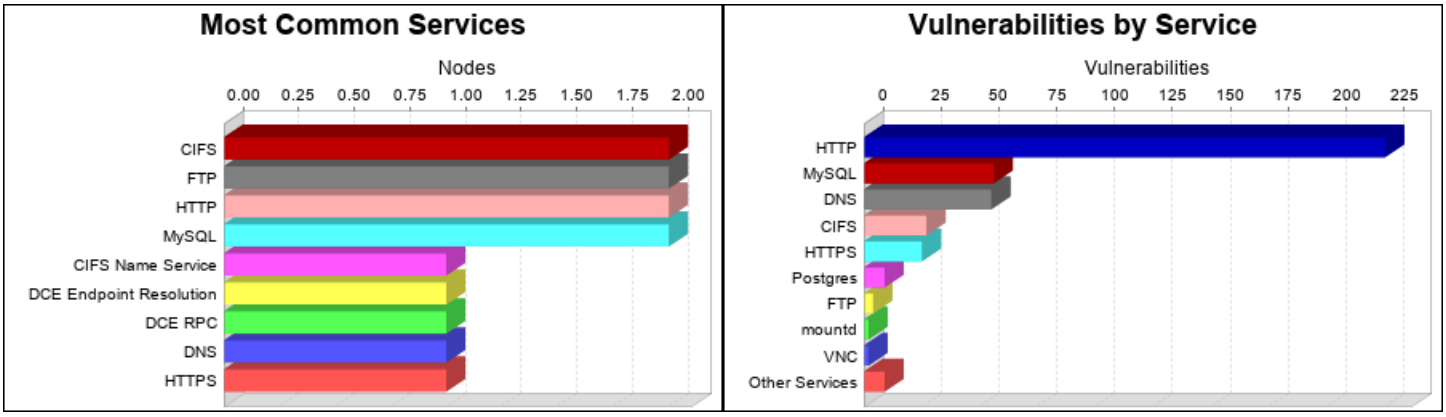
There were 4 occurrences of the cifs-smb-signing-disabled and cifs-smb-signing-not-required vulnerabilities, making them the most common vulnerabilities. There were 243 vulnerability instances in the Denial of Service category, making it the most common vulnerability category.



The cifs-smb-signing-disabled vulnerability poses the highest risk to the organization with a risk score of 3,298. Risk scores are based on the types and numbers of vulnerabilities on affected assets.
There were 2 operating systems identified during this scan.



The Microsoft Windows and Ubuntu Linux operating systems were found on 1 systems, making them the most common operating systems.
There were 24 services found to be running during this scan.



The CIFS, FTP, HTTP and MySQL services were found on 2 systems, making them the most common services. The HTTP service was found to have the most vulnerabilities during this scan with 225 vulnerabilities.

2. Discovered Systems

Node	Operating System	Risk	Aliases
192.168.234.131	Ubuntu Linux 8.04	250,137	•metasploitable •metasploitable.localdomain
192.168.234.130	Microsoft Windows 7 Ultimate Edition SP1	11,910	•SKIF-PC

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

3.1.1. Apache HTTPD: APR apr_palloc heap overflow (CVE-2009-2412) (apache-httpd-cve-2009-2412)

Description:

The affected asset is vulnerable to this vulnerability ONLY if a non-Apache application can be passed unsanitized user-provided sizes to the apr_palloc() function. Review your web server configuration for validation. A flaw in apr_palloc() in the bundled copy of APR could cause heap overflows in programs that try to apr_palloc() a user controlled size. The Apache HTTP Server itself does not pass unsanitized user-provided sizes to this function, so it could only be triggered through some other application which uses apr_palloc() in a vulnerable way.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2009-11-09-1
BID	35949
CVE	CVE-2009-2412
OVAL	8394
OVAL	9958
SUSE	SUSE-SA:2009:050
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.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 < 2.2.13

Upgrade to Apache HTTPD version 2.2.13

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.13.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.

3.1.2. Obsolete Version of Apache HTTPD (apache-httpd-obsolete)

Description:

Older versions of Apache HTTPD (prior to 2.4.X) are no longer officially supported. There may exist unreported vulnerabilities for these versions. An upgrade to the latest version should be applied to mitigate these unknown risks.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
URL	https://en.wikipedia.org/wiki/Apache_HTTP_Server
URL	https://httpd.apache.org

Vulnerability Solution:

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.30.tar.gz
The latest version of Apache HTTPD is 2.4.30.
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.

3.1.3. 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:
192.168.234.131:8180	Running HTTP serviceProduct Tomcat exists -- Apache TomcatBased on the following 2 results:HTTP GET request to http://192.168.234.131:8180/manager/html HTTP response code was an expected 401 HTTP GET request to http://192.168.234.131:8180/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

3.1.4. Samba NDR Parsing Heap Overflow Vulnerability (cifs-samba-ms-rpc-bof)

Description:

Multiple heap-based buffer overflows in the NDR parsing in smbd in Samba 3.0.0 through 3.0.25rc3 allow remote attackers to execute arbitrary code via crafted MS-RPC requests involving (1) DFSEnum (netdfs_io_dfs_EnumInfo_d), (2) RFNPCNEX (smb_io_notify_option_type_data), (3) LsarAddPrivilegesToAccount (lsa_io_privilege_set), (4) NetSetFileSecurity (sec_io_acl), or (5) LsarLookupSids/LsarLookupSids2 (lsa_io_trans_names).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:139	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian
192.168.234.131:445	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-2007-07-31
BID	23973
BID	24195
BID	24196
BID	24197
BID	24198
BID	25159
CERT-VN	773720
CVE	CVE-2007-2446
DEBIAN	DSA-1291
OVAL	11415
REDHAT	RHSA-2007:0354
SUSE	SUSE-SA:2007:031
URL	http://www.samba.org/samba/security/CVE-2007-2446.html
XF	34309
XF	34311
XF	34312
XF	34314
XF	34316

Vulnerability Solution:

Samba < 3.0.25

Download and apply the upgrade from: https://ftp.samba.org/pub/samba/stable/samba-3.0.25.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.

3.1.5. 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:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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.

3.1.6. PHP Multiple Vulnerabilities Fixed in version 5.2.12 (http-php-multiple-vulns-5-2-12)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1

Source	Reference
BID	37389
BID	37390
CVE	CVE-2009-3557
CVE	CVE-2009-3558
CVE	CVE-2009-4017
CVE	CVE-2009-4142
CVE	CVE-2009-4143
DEBIAN	DSA-1940
DEBIAN	DSA-2001
OVAL	10005
OVAL	10483
OVAL	6667
OVAL	7085
OVAL	7396
OVAL	7439
URL	http://www.php.net/ChangeLog-5.php#5.2.12
URL	http://www.php.net/releases/5_2_12.php
XF	54455

Vulnerability Solution:

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

3.1.7. PHP Multiple Vulnerabilities Fixed in version 5.2.6 (http-php-multiple-vulns-5-2-6)

Description:

The escapeshellcmd API function in PHP before 5.2.6 has unknown impact and context-dependent attack vectors related to "incomplete multibyte chars."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2008-07-31
BID	29009
CVE	CVE-2008-2050
CVE	CVE-2008-2051
CVE	CVE-2008-2107
CVE	CVE-2008-2108
DEBIAN	DSA-1572
DEBIAN	DSA-1578
DEBIAN	DSA-1789
OVAL	10256
OVAL	10644
OVAL	10844
REDHAT	RHSA-2008:0505
REDHAT	RHSA-2008:0544
REDHAT	RHSA-2008:0545
REDHAT	RHSA-2008:0546
REDHAT	RHSA-2008:0582
XF	42133
XF	42226
XF	42284

Vulnerability Solution:

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

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

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8

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

References:

Source	Reference
APPLE	APPLE-SA-2008-10-09
APPLE	APPLE-SA-2009-05-12
BID	30087
BID	31681
BID	32383
BID	32625
BID	32673
BID	32688
BID	32948
CERT	TA09-133A
CVE	CVE-2008-2371
CVE	CVE-2008-5557
CVE	CVE-2008-5624
CVE	CVE-2008-5625
CVE	CVE-2008-5658
CVE	CVE-2008-5844
DEBIAN	DSA-1602
DEBIAN	DSA-1789
OVAL	10286
REDHAT	RHSA-2009:0350
URL	http://bugs.php.net/bug.php?id=42718
URL	http://bugs.php.net/bug.php?id=45722
URL	http://www.php.net/ChangeLog-5.php#5.2.8
XF	47079
XF	47314
XF	47318
XF	47525

Vulnerability Solution:

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

3.1.9. MySQL Obsolete Version (mysql-obsolete-version)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

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

Vulnerability Solution:

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

3.1.10. PHP Vulnerability: CVE-2008-0599 (php-cve-2008-0599)

Description:

The init_request_info function in sapi/cgi/cgi_main.c in PHP before 5.2.6 does not properly consider operator precedence when calculating the length of PATH_TRANSLATED, which might allow remote attackers to execute arbitrary code via a crafted URI.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2008-07-31
BID	29009
CERT-VN	147027
CVE	CVE-2008-0599

Source	Reference
OVAL	5510
REDHAT	RHSA-2008:0505
XF	42137

Vulnerability Solution:

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

3.1.11. PHP Vulnerability: CVE-2008-2050 (php-cve-2008-2050)

Description:

Stack-based buffer overflow in the FastCGI SAPI (fastcgi.c) in PHP before 5.2.6 has unknown impact and attack vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2008-07-31
BID	29009
CVE	CVE-2008-2050
DEBIAN	DSA-1572
URL	http://www.php.net/ChangeLog-5.php
XF	42133

Vulnerability Solution:

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

3.1.12. PHP Vulnerability: CVE-2008-2051 (php-cve-2008-2051)

Description:

The escapeshellcmd API function in PHP before 5.2.6 has unknown impact and context-dependent attack vectors related to "incomplete multibyte chars."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2008-07-31
BID	29009
CVE	CVE-2008-2051
DEBIAN	DSA-1572
DEBIAN	DSA-1578
OVAL	10256
REDHAT	RHSA-2008:0505
REDHAT	RHSA-2008:0544
REDHAT	RHSA-2008:0545
REDHAT	RHSA-2008:0546
REDHAT	RHSA-2008:0582

Vulnerability Solution:

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

3.1.13. PHP Vulnerability: CVE-2008-5557 (php-cve-2008-5557)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-05-12

Source	Reference
BID	32948
CERT	TA09-133A
CVE	CVE-2008-5557
DEBIAN	DSA-1789
OVAL	10286
REDHAT	RHSA-2009:0350
XF	47525

Vulnerability Solution:

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

3.1.14. PHP Vulnerability: CVE-2009-4143 (php-cve-2009-4143)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
BID	37390
CVE	CVE-2009-4143
DEBIAN	DSA-2001
OVAL	7439
URL	http://www.php.net/releases/5_2_12.php

Vulnerability Solution:

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

3.1.15. PHP Vulnerability: CVE-2012-2688 (php-cve-2012-2688)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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/

3.1.16. PHP Vulnerability: CVE-2015-4599 (php-cve-2015-4599)

Description:

The SoapFault::__toString method in ext/soap/soap.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information, cause a denial of service (application crash), or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	75251
CVE	CVE-2015-4599
REDHAT	RHSA-2015:1135
REDHAT	RHSA-2015:1218

Vulnerability Solution:

•Upgrade to PHP version 5.4.40

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

•Upgrade to PHP version 5.5.24

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

•Upgrade to PHP version 5.6.8

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

3.1.17. PHP Vulnerability: CVE-2015-4600 (php-cve-2015-4600)

Description:

The SoapClient implementation in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to "type confusion" issues in the (1) SoapClient::__getLastRequest, (2) SoapClient::__getLastResponse, (3) SoapClient::__getLastRequestHeaders, (4) SoapClient::__getLastResponseHeaders, (5) SoapClient::__getCookies, and (6) SoapClient::__setCookie methods.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	74413
CVE	CVE-2015-4600
REDHAT	RHSA-2015:1135
REDHAT	RHSA-2015:1218

Vulnerability Solution:

•Upgrade to PHP version 5.4.40

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

•Upgrade to PHP version 5.5.24

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

•Upgrade to PHP version 5.6.8

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

3.1.18. PHP Vulnerability: CVE-2015-4601 (php-cve-2015-4601)

Description:

PHP before 5.6.7 might allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to "type confusion" issues in (1) ext/soap/php_encoding.c, (2) ext/soap/php_http.c, and (3) ext/soap/soap.c, a different issue than CVE-2015-4600.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	75246
CVE	CVE-2015-4601
REDHAT	RHSA-2015:1135
REDHAT	RHSA-2015:1218

Vulnerability Solution:

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

3.1.19. PHP Vulnerability: CVE-2015-4602 (php-cve-2015-4602)

Description:

The __PHP_Incomplete_Class function in ext/standard/incomplete_class.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	75249
CVE	CVE-2015-4602
REDHAT	RHSA-2015:1135
REDHAT	RHSA-2015:1186
REDHAT	RHSA-2015:1187
REDHAT	RHSA-2015:1218

Vulnerability Solution:

•Upgrade to PHP version 5.4.40

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

•Upgrade to PHP version 5.5.24

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

•Upgrade to PHP version 5.6.8

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

3.1.20. PHP Vulnerability: CVE-2015-4603 (php-cve-2015-4603)

Description:

The exception::getTraceAsString function in Zend/zend_exceptions.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to execute arbitrary code via an unexpected data type, related to a "type confusion" issue.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	75252
CVE	CVE-2015-4603
REDHAT	RHSA-2015:1135
REDHAT	RHSA-2015:1186
REDHAT	RHSA-2015:1187
REDHAT	RHSA-2015:1218

Vulnerability Solution:

•Upgrade to PHP version 5.4.40

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

•Upgrade to PHP version 5.5.24

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

•Upgrade to PHP version 5.6.8

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

3.1.21. PHP Vulnerability: CVE-2015-5589 (php-cve-2015-5589)

Description:

The phar_convert_to_other function in ext/phar/phar_object.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 does not validate a file pointer before a close operation, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted TAR archive that is mishandled in a Phar::convertToData call.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	75974
CVE	CVE-2015-5589
DEBIAN	DSA-3344

Vulnerability Solution:

•Upgrade to PHP version 5.4.43

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

•Upgrade to PHP version 5.5.27

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

•Upgrade to PHP version 5.6.11

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

3.1.22. PHP Fixed security issue (php-fixed-security-issue)

Description:

The init_request_info function in sapi/cgi/cgi_main.c in PHP before 5.2.6 does not properly consider operator precedence when calculating the length of PATH_TRANSLATED, which might allow remote attackers to execute arbitrary code via a crafted URI.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2008-07-31
BID	29009
CERT-VN	147027
CVE	CVE-2008-0599
OVAL	5510
REDHAT	RHSA-2008:0505
XF	42137

Vulnerability Solution:

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

3.1.23. Shell Backdoor Service (shell-backdoor)

Description:

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

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:1524	Running Shell Backdoor service

References:

None

Vulnerability Solution:

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

3.1.24. Obsolete Version of Ubuntu (ubuntu-obsolete-version)

Description:

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

Affected Nodes:

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

References:

None

Vulnerability Solution:

Upgrade to a supported version of Ubuntu Linux

3.1.25. VMware Player: Hosted products DHCP security vulnerabilities addressed (VMSA-2007-0006) (CVE-2007-0061) (vmsa-2007-0006-cve-2007-0061-player)

Description:

The DHCP server in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 55017, Player before 1.0.5 Build 56455 and Player 2 before 2.0.1 Build 55017, ACE before 1.0.3 Build 54075 and ACE 2 before 2.0.1 Build 55017, and Server before 1.0.4 Build 56528 allows remote attackers to execute arbitrary code via a malformed packet that triggers "corrupt stack memory."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	25729
CVE	CVE-2007-0061
URL	http://www.vmware.com/security/advisories/VMSA-2007-0006.html
XF	33101

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.5

Upgrade to VMware Player version 1.0.5

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.0 and < 2.0.1

Upgrade to VMware Player version 2.0.1

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.26. VMware Workstation: Hosted products DHCP security vulnerabilities addressed (VMSA-2007-0006) (CVE-2007-0061) (vmsa-2007-0006-cve-2007-0061-workstation)

Description:

The DHCP server in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 55017, Player before 1.0.5 Build 56455 and Player 2 before 2.0.1 Build 55017, ACE before 1.0.3 Build 54075 and ACE 2 before 2.0.1 Build 55017, and Server before 1.0.4 Build 56528 allows remote attackers to execute arbitrary code via a malformed packet that triggers "corrupt stack memory."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	25729
CVE	CVE-2007-0061
URL	http://www.vmware.com/security/advisories/VMSA-2007-0006.html
XF	33101

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.5

Upgrade to VMware Workstation version 5.5.5

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6 and < 6.0.1

Upgrade to VMware Workstation version 6.0.1

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.1.27. VMware Player: Hosted products DHCP security vulnerabilities addressed (VMSA-2007-0006) (CVE-2007-0062) (vmsa-2007-0006-cve-2007-0062-player)

Description:

Integer overflow in the ISC dhcpd 3.0.x before 3.0.7 and 3.1.x before 3.1.1; and the DHCP server in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 55017, Player before 1.0.5 Build 56455 and Player 2 before 2.0.1 Build 55017, ACE before 1.0.3 Build 54075 and ACE 2 before 2.0.1 Build 55017, and Server before 1.0.4 Build 56528; allows remote attackers to cause a denial of service (daemon crash) or execute arbitrary code via a malformed DHCP packet with a large dhcp-max-message-size that triggers a stack-based buffer overflow, related to servers configured to send many DHCP options to clients.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	25729
CVE	CVE-2007-0062
URL	http://www.vmware.com/security/advisories/VMSA-2007-0006.html
XF	33102

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.5

Upgrade to VMware Player version 1.0.5

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.0 and < 2.0.1

Upgrade to VMware Player version 2.0.1

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.28. VMware Workstation: Hosted products DHCP security vulnerabilities addressed (VMSA-2007-0006) (CVE-2007-0062) (vmsa-2007-0006-cve-2007-0062-workstation)

Description:

Integer overflow in the ISC dhcpd 3.0.x before 3.0.7 and 3.1.x before 3.1.1; and the DHCP server in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 55017, Player before 1.0.5 Build 56455 and Player 2 before 2.0.1 Build 55017, ACE before 1.0.3 Build 54075 and ACE 2 before 2.0.1 Build 55017, and Server before 1.0.4 Build 56528; allows remote attackers to cause a denial of service (daemon crash) or execute arbitrary code via a malformed DHCP packet with a large dhcp-max-message-size that triggers a stack-based buffer overflow, related to servers configured to send many DHCP options to clients.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	25729

Source	Reference
CVE	CVE-2007-0062
URL	http://www.vmware.com/security/advisories/VMSA-2007-0006.html
XF	33102

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.5

Upgrade to VMware Workstation version 5.5.5

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6 and < 6.0.1

Upgrade to VMware Workstation version 6.0.1

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.1.29. VMware Player: Hosted products DHCP security vulnerabilities addressed (VMSA-2007-0006) (CVE-2007-0063) (vmsa-2007-0006-cve-2007-0063-player)

Description:

Integer underflow in the DHCP server in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 55017, Player before 1.0.5 Build 56455 and Player 2 before 2.0.1 Build 55017, ACE before 1.0.3 Build 54075 and ACE 2 before 2.0.1 Build 55017, and Server before 1.0.4 Build 56528 allows remote attackers to execute arbitrary code via a malformed DHCP packet that triggers a stack-based buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	25729
CVE	CVE-2007-0063
URL	http://www.vmware.com/security/advisories/VMSA-2007-0006.html
XF	33103

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.5

Upgrade to VMware Player version 1.0.5

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.0 and < 2.0.1

Upgrade to VMware Player version 2.0.1

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.30. VMware Workstation: Hosted products DHCP security vulnerabilities addressed (VMSA-2007-0006) (CVE-2007-0063) (vmsa-2007-0006-cve-2007-0063-workstation)

Description:

Integer underflow in the DHCP server in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 55017, Player before 1.0.5 Build 56455 and Player 2 before 2.0.1 Build 55017, ACE before 1.0.3 Build 54075 and ACE 2 before 2.0.1 Build 55017, and Server before 1.0.4 Build 56528 allows remote attackers to execute arbitrary code via a malformed DHCP packet that triggers a stack-based buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	25729
CVE	CVE-2007-0063
URL	http://www.vmware.com/security/advisories/VMSA-2007-0006.html
XF	33103

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.5

Upgrade to VMware Workstation version 5.5.5

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6 and < 6.0.1

Upgrade to VMware Workstation version 6.0.1

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.1.31. Obsolete Version of VMware Player (vmware-player-obsolete)

Description:

VMware Player versions prior to 12.0 are no longer supported and may contain unpatched security flaws. It is recommended to upgrade to the latest version.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
URL	http://www.vmware.com/support/policies/personal-desktop/eol.html

Vulnerability Solution:

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.32. Obsolete Version of VMware Workstation (vmware-workstation-obsolete)

Description:

VMware Workstation versions prior to 11.0 are no longer supported and may contain unpatched security flaws. It is recommended to upgrade to the latest version. End of general support for VMware Workstation 11.x is scheduled for 2016/06/02.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
URL	https://www.vmware.com/files/pdf/support/Product-Lifecycle-Matrix.pdf

Vulnerability Solution:

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/14_0

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

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:5900	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.

3.1.34. Samba GETDC Mailslot Processing Buffer Overflow In Nmbd (cifs-samba-nmbd-getdc-mailslot-bof)

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:
192.168.234.131:139	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian
192.168.234.131:445	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-2007-12-17
BID	26454
CERT	TA07-352A
CVE	CVE-2007-4572
DEBIAN	DSA-1409
OVAL	11132
OVAL	5643
REDHAT	RHSA-2007:1013
REDHAT	RHSA-2007:1016
REDHAT	RHSA-2007:1017
SUSE	SUSE-SA:2007:065
URL	http://www.samba.org/samba/security/CVE-2007-4572.html
XF	38501

Vulnerability Solution:

Samba < 3.0.27

Download and apply the upgrade from: https://ftp.samba.org/pub/samba/stable/samba-3.0.27.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.

3.1.35. Samba 'reply_netbios_packet' Nmbd Buffer Overflow (cifs-samba-reply-netbios-packet-bof)

Description:

Stack-based buffer overflow in the reply_netbios_packet function in nmbd/nmbd_packets.c in nmbd in Samba 3.0.0 through 3.0.26a, when operating as a WINS server, allows remote attackers to execute arbitrary code via crafted WINS Name Registration requests followed by a WINS Name Query request.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:139	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian
192.168.234.131:445	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-2007-12-17
BID	26455
CERT	TA07-352A
CVE	CVE-2007-5398
DEBIAN	DSA-1409
OVAL	10230
OVAL	5811
REDHAT	RHSA-2007:1013
REDHAT	RHSA-2007:1016
REDHAT	RHSA-2007:1017
SUSE	SUSE-SA:2007:065
URL	http://www.samba.org/samba/security/CVE-2007-5398.html
XF	38502

Vulnerability Solution:

Samba < 3.0.27

Download and apply the upgrade from: https://ftp.samba.org/pub/samba/stable/samba-3.0.27.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.

3.1.36. Samba send_mailslot GETDC Buffer Overflow (cifs-samba-send-mailslot-bof)

Description:

Stack-based buffer overflow in the send_mailslot function in nmbd in Samba 3.0.0 through 3.0.27a, when the "domain logons" option is enabled, allows remote attackers to execute arbitrary code via a GETDC mailslot request composed of a long GETDC string following an offset username in a SAMLOGON logon request.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:139	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian
192.168.234.131:445	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-2008-02-11
BID	26791
CERT	TA08-043B
CERT-VN	438395
CVE	CVE-2007-6015
DEBIAN	DSA-1427
OVAL	11572
OVAL	5605
REDHAT	RHSA-2007:1114
REDHAT	RHSA-2007:1117
SUSE	SUSE-SA:2007:068
URL	http://www.samba.org/samba/security/CVE-2007-6015.html
XF	38965

Vulnerability Solution:

Samba < 3.0.28

Download and apply the upgrade from: https://ftp.samba.org/pub/samba/stable/samba-3.0.28.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.

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

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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.

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

Description:

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

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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
URL	https://kb.isc.org/article/AA-00913/0/BIND-9-Security-Vulnerability-Matrix.html
URL	https://www.isc.org/software/bind

Vulnerability Solution:

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

3.1.39. MySQL dispatch_command() Multiple Format String Vulnerabilities (mysql-dispatch_command-multiple-format-string)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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-2010-03-29-1
BID	35609
CVE	CVE-2009-2446
OVAL	11857
REDHAT	RHSA-2009:1289
REDHAT	RHSA-2010:0110
XF	51614

Vulnerability Solution:

Oracle MySQL >= 5.0 and < 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.

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

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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

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

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:512	Running Remote Execution service

References:

None

Vulnerability Solution:

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

3.1.42. VMware Player: VNnc Codec Heap Overflow vulnerabilities (VMSA-2009-0005) (CVE-2009-0909) (vmsa-2009-0005-cve-2009-0909-player)

Description:

Heap-based buffer overflow in the VNnc Codec in VMware Workstation 6.5.x before 6.5.2 build 156735, VMware Player 2.5.x before 2.5.2 build 156735, VMware ACE 2.5.x before 2.5.2 build 156735, and VMware Server 2.0.x before 2.0.1 build 156745 allows remote attackers to execute arbitrary code via a crafted web page or video file, aka ZDI-CAN-435.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	34373
CVE	CVE-2009-0909
OVAL	6251
URL	http://www.vmware.com/security/advisories/VMSA-2009-0005.html

Vulnerability Solution:

VMware Player >= 2.5 and < 2.5.2
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.43. VMware Workstation: VNnc Codec Heap Overflow vulnerabilities (VMSA-2009-0005) (CVE-2009-0909) (vmsa-2009-0005-cve-2009-0909-workstation)

Description:

Heap-based buffer overflow in the VNnc Codec in VMware Workstation 6.5.x before 6.5.2 build 156735, VMware Player 2.5.x before 2.5.2 build 156735, VMware ACE 2.5.x before 2.5.2 build 156735, and VMware Server 2.0.x before 2.0.1 build 156745 allows remote attackers to execute arbitrary code via a crafted web page or video file, aka ZDI-CAN-435.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	34373
CVE	CVE-2009-0909
OVAL	6251
URL	http://www.vmware.com/security/advisories/VMSA-2009-0005.html

Vulnerability Solution:
VMware Workstation >= 6.5 and < 6.5.2
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

3.1.44. VMware Player: VMware VMnc Codec heap overflow vulnerabilities (VMSA-2010-0007) (CVE-2009-1564) (vmsa-2010-0007-cve-2009-1564-player)

Description:

Heap-based buffer overflow in vmnc.dll in the VMnc media codec in VMware Movie Decoder before 6.5.4 Build 246459 on Windows, and the movie decoder in VMware Workstation 6.5.x before 6.5.4 build 246459, VMware Player 2.5.x before 2.5.4 build 246459, and VMware Server 2.x on Windows, allows remote attackers to execute arbitrary code via an AVI file with crafted video chunks that use HexTile encoding.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference

Source	Reference
BID	39363
CVE	CVE-2009-1564
DISA_SEVERITY	Category I
DISA_VMSKEY	V0023997
IAVM	2010-A-0066
URL	http://www.vmware.com/security/advisories/VMSA-2010-0007.html

Vulnerability Solution:

VMware Player >= 2.5 and < 2.5.4
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.45. VMware Workstation: VMware VMnc Codec heap overflow vulnerabilities (VMSA-2010-0007) (CVE-2009-1564) (vmsa-2010-0007-cve-2009-1564-workstation)

Description:

Heap-based buffer overflow in vmnc.dll in the VMnc media codec in VMware Movie Decoder before 6.5.4 Build 246459 on Windows, and the movie decoder in VMware Workstation 6.5.x before 6.5.4 build 246459, VMware Player 2.5.x before 2.5.4 build 246459, and VMware Server 2.x on Windows, allows remote attackers to execute arbitrary code via an AVI file with crafted video chunks that use HexTile encoding.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	39363
CVE	CVE-2009-1564
DISA_SEVERITY	Category I
DISA_VMSKEY	V0023997
IAVM	2010-A-0066
URL	http://www.vmware.com/security/advisories/VMSA-2010-0007.html

Vulnerability Solution:

VMware Workstation >= 6.5 and < 6.5.4
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

3.1.46. VMware Player: VMware VMnc Codec heap overflow vulnerabilities (VMSA-2010-0007) (CVE-2009-1565) (vmsa-2010-0007-cve-2009-1565-player)

Description:

vmnc.dll in the VMnc media codec in VMware Movie Decoder before 6.5.4 Build 246459 on Windows, and the movie decoder in VMware Workstation 6.5.x before 6.5.4 build 246459, VMware Player 2.5.x before 2.5.4 build 246459, and VMware Server 2.x on Windows, allows remote attackers to execute arbitrary code via an AVI file with crafted HexTile-encoded video chunks that trigger heap-based buffer overflows, related to "integer truncation errors."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	39364
CVE	CVE-2009-1565
DISA_SEVERITY	Category I
DISA_VMSKEY	V0023997
IAVM	2010-A-0066
URL	http://www.vmware.com/security/advisories/VMSA-2010-0007.html

Vulnerability Solution:

VMware Player >= 2.5 and < 2.5.4
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.47. VMware Workstation: VMware VMnc Codec heap overflow vulnerabilities (VMSA-2010-0007) (CVE-2009-1565) (vmsa-2010-0007-cve-2009-1565-workstation)

Description:

vmnc.dll in the VMnc media codec in VMware Movie Decoder before 6.5.4 Build 246459 on Windows, and the movie decoder in VMware Workstation 6.5.x before 6.5.4 build 246459, VMware Player 2.5.x before 2.5.4 build 246459, and VMware Server 2.x on Windows, allows remote attackers to execute arbitrary code via an AVI file with crafted HexTile-encoded video chunks that trigger heap-based buffer overflows, related to "integer truncation errors."

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	39364
CVE	CVE-2009-1565
DISA_SEVERITY	Category I
DISA_VMSKEY	V0023997
IAVM	2010-A-0066
URL	http://www.vmware.com/security/advisories/VMSA-2010-0007.html

Vulnerability Solution:

VMware Workstation >= 6.5 and < 6.5.4
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

3.1.48. VMware Player: Windows-based VMware Tools Unsafe Library Loading vulnerability (VMSA-2010-0007) (CVE-2010-1141) (vmsa-2010-0007-cve-2010-1141-player)

Description:

VMware Tools in VMware Workstation 6.5.x before 6.5.4 build 246459; VMware Player 2.5.x before 2.5.4 build 246459; VMware ACE 2.5.x before 2.5.4 build 246459; VMware Server 2.x before 2.0.2 build 203138; VMware Fusion 2.x before 2.0.6 build 246742; VMware ESXi 3.5 and 4.0; and VMware ESX 2.5.5, 3.0.3, 3.5, and 4.0 does not properly access libraries, which allows user-assisted remote attackers to execute arbitrary code by tricking a Windows guest OS user into clicking on a file that is stored on a network share.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
CVE	CVE-2010-1141
DISA_SEVERITY	Category I
DISA_VMSKEY	V0023997
IAVM	2010-A-0066
OVAL	7020
URL	http://www.vmware.com/security/advisories/VMSA-2010-0007.html

Vulnerability Solution:

VMware Player >= 2.5 and < 2.5.4
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.49. VMware Workstation: Windows-based VMware Tools Unsafe Library Loading vulnerability (VMSA-2010-0007) (CVE-2010-1141) (vmsa-2010-0007-cve-2010-1141-workstation)

Description:

VMware Tools in VMware Workstation 6.5.x before 6.5.4 build 246459; VMware Player 2.5.x before 2.5.4 build 246459; VMware ACE 2.5.x before 2.5.4 build 246459; VMware Server 2.x before 2.0.2 build 203138; VMware Fusion 2.x before 2.0.6 build 246742; VMware ESXi 3.5 and 4.0; and VMware ESX 2.5.5, 3.0.3, 3.5, and 4.0 does not properly access libraries, which allows user-assisted remote attackers to execute arbitrary code by tricking a Windows guest OS user into clicking on a file that is stored on a network share.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
CVE	CVE-2010-1141
DISA_SEVERITY	Category I
DISA_VMSKEY	V0023997
IAVM	2010-A-0066
OVAL	7020
URL	http://www.vmware.com/security/advisories/VMSA-2010-0007.html

Vulnerability Solution:

VMware Workstation >= 6.5 and < 6.5.4
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

3.1.50. VMware Player: Windows-based VMware Tools Arbitrary Code Execution vulnerability (VMSA-2010-0007) (CVE-2010-1142) (vmsa-2010-0007-cve-2010-1142-player)

Description:

VMware Tools in VMware Workstation 6.5.x before 6.5.4 build 246459; VMware Player 2.5.x before 2.5.4 build 246459; VMware ACE 2.5.x before 2.5.4 build 246459; VMware Server 2.x before 2.0.2 build 203138; VMware Fusion 2.x before 2.0.6 build 246742; VMware ESXi 3.5 and 4.0; and VMware ESX 2.5.5, 3.0.3, 3.5, and 4.0 does not properly load VMware programs, which might allow Windows guest OS users to gain privileges by placing a Trojan horse program at an unspecified location on the guest OS disk.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	39394
CVE	CVE-2010-1142
DISA_SEVERITY	Category I
DISA_VMSKEY	V0023997
IAVM	2010-A-0066
URL	http://www.vmware.com/security/advisories/VMSA-2010-0007.html

Vulnerability Solution:

VMware Player >= 2.5 and < 2.5.4
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.51. VMware Workstation: Windows-based VMware Tools Arbitrary Code Execution vulnerability (VMSA-2010-0007) (CVE-2010-1142) (vmsa-2010-0007-cve-2010-1142-workstation)

Description:

VMware Tools in VMware Workstation 6.5.x before 6.5.4 build 246459; VMware Player 2.5.x before 2.5.4 build 246459; VMware ACE 2.5.x before 2.5.4 build 246459; VMware Server 2.x before 2.0.2 build 203138; VMware Fusion 2.x before 2.0.6 build 246742; VMware ESXi 3.5 and 4.0; and VMware ESX 2.5.5, 3.0.3, 3.5, and 4.0 does not properly load VMware programs, which might allow Windows guest OS users to gain privileges by placing a Trojan horse program at an unspecified location on the guest OS disk.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	39394
CVE	CVE-2010-1142
DISA_SEVERITY	Category I
DISA_VMSKEY	V0023997
IAVM	2010-A-0066

Source	Reference
URL	http://www.vmware.com/security/advisories/VMSA-2010-0007.html

Vulnerability Solution:

VMware Workstation >= 6.5 and < 6.5.4
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

3.1.52. VMware Player: UDF file system import remote code execution (VMSA-2011-0011) (CVE-2011-3868) (vmsa-2011-0011-cve-2011-3868-player)

Description:

Buffer overflow in VMware Workstation 7.x before 7.1.5, VMware Player 3.x before 3.1.5, VMware Fusion 3.1.x before 3.1.3, and VMware AMS allows remote attackers to execute arbitrary code via a crafted UDF filesystem in an ISO image.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	49942
CVE	CVE-2011-3868
URL	http://www.vmware.com/security/advisories/VMSA-2011-0011.html

Vulnerability Solution:

VMware Player >= 3.1 and < 3.1.5
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.53. VMware Workstation: UDF file system import remote code execution (VMSA-2011-0011) (CVE-2011-3868) (vmsa-2011-0011-cve-2011-3868-workstation)

Description:

Buffer overflow in VMware Workstation 7.x before 7.1.5, VMware Player 3.x before 3.1.5, VMware Fusion 3.1.x before 3.1.3, and VMware AMS allows remote attackers to execute arbitrary code via a crafted UDF filesystem in an ISO image.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	49942
CVE	CVE-2011-3868
URL	http://www.vmware.com/security/advisories/VMSA-2011-0011.html

Vulnerability Solution:

VMware Workstation >= 7 and < 7.1.5
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.1.54. VMware Player: VMware host memory overwrite vulnerability (data pointers) (VMSA-2012-0009) (CVE-2012-1516) (vmsa-2012-0009-cve-2012-1516-player)

Description:

The VMX process in VMware ESXi 3.5 through 4.1 and ESX 3.5 through 4.1 does not properly handle RPC commands, which allows guest OS users to cause a denial of service (memory overwrite and process crash) or possibly execute arbitrary code on the host OS via vectors involving data pointers.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	53369
CVE	CVE-2012-1516
DISA_SEVERITY	Category I
DISA_VMSKEY	V0032167
DISA_VMSKEY	V0032171
IAVM	2012-A-0072
IAVM	2012-A-0073
OVAL	16810
URL	http://www.vmware.com/security/advisories/VMSA-2012-0009.html
XF	75373

Vulnerability Solution:

VMware Player >= 3.1 and < 3.1.6

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.55. VMware Workstation: VMware host memory overwrite vulnerability (data pointers) (VMSA-2012-0009) (CVE-2012-1516) (vmsa-2012-0009-cve-2012-1516-workstation)

Description:

The VMX process in VMware ESXi 3.5 through 4.1 and ESX 3.5 through 4.1 does not properly handle RPC commands, which allows guest OS users to cause a denial of service (memory overwrite and process crash) or possibly execute arbitrary code on the host OS via vectors involving data pointers.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	53369
CVE	CVE-2012-1516
DISA_SEVERITY	Category I
DISA_VMSKEY	V0032167
DISA_VMSKEY	V0032171
IAVM	2012-A-0072
IAVM	2012-A-0073
OVAL	16810
URL	http://www.vmware.com/security/advisories/VMSA-2012-0009.html
XF	75373

Vulnerability Solution:

VMware Workstation >= 7 and < 7.1.5
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.1.56. VMware Player: VMware host memory overwrite vulnerability (function pointers) (VMSA-2012-0009) (CVE-2012-1517) (vmsa-2012-0009-cve-2012-1517-player)

Description:

The VMX process in VMware ESXi 4.1 and ESX 4.1 does not properly handle RPC commands, which allows guest OS users to cause a denial of service (memory overwrite and process crash) or possibly execute arbitrary code on the host OS via vectors involving function pointers.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	53369
CVE	CVE-2012-1517
DISA_SEVERITY	Category I
IAVM	2012-A-0073
OSVDB	81692
OVAL	17231
URL	http://www.vmware.com/security/advisories/VMSA-2012-0009.html
XF	75374

Vulnerability Solution:

VMware Player >= 3.1 and < 3.1.6
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.57. VMware Workstation: VMware host memory overwrite vulnerability (function pointers) (VMSA-2012-0009) (CVE-2012-1517) (vmsa-2012-0009-cve-2012-1517-workstation)

Description:

The VMX process in VMware ESXi 4.1 and ESX 4.1 does not properly handle RPC commands, which allows guest OS users to cause a denial of service (memory overwrite and process crash) or possibly execute arbitrary code on the host OS via vectors involving function pointers.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	53369
CVE	CVE-2012-1517

Source	Reference
DISA_SEVERITY	Category I
IAVM	2012-A-0073
OSVDB	81692
OVAL	17231
URL	http://www.vmware.com/security/advisories/VMSA-2012-0009.html
XF	75374

Vulnerability Solution:

VMware Workstation >= 7 and < 7.1.6
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.1.58. VMware Player: VMware SCSI device unchecked memory write (VMSA-2012-0009) (CVE-2012-2450) (vmsa-2012-0009-cve-2012-2450-player)

Description:

VMware Workstation 8.x before 8.0.3, VMware Player 4.x before 4.0.3, VMware Fusion 4.x before 4.1.2, VMware ESXi 3.5 through 5.0, and VMware ESX 3.5 through 4.1 do not properly register SCSI devices, which allows guest OS users to cause a denial of service (invalid write operation and VMX process crash) or possibly execute arbitrary code on the host OS by leveraging administrative privileges on the guest OS.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	53369
CVE	CVE-2012-2450
DISA_SEVERITY	Category I
DISA_VMSKEY	V0032167
DISA_VMSKEY	V0032171
IAVM	2012-A-0072
IAVM	2012-A-0073
OSVDB	81695
OVAL	16852
URL	http://www.vmware.com/security/advisories/VMSA-2012-0009.html

Source	Reference
XF	75377

Vulnerability Solution:

VMware Player >= 3.1 and < 3.1.6
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.59. VMware Workstation: VMware SCSI device unchecked memory write (VMSA-2012-0009) (CVE-2012-2450) (vmsa-2012-0009-cve-2012-2450-workstation)

Description:

VMware Workstation 8.x before 8.0.3, VMware Player 4.x before 4.0.3, VMware Fusion 4.x before 4.1.2, VMware ESXi 3.5 through 5.0, and VMware ESX 3.5 through 4.1 do not properly register SCSI devices, which allows guest OS users to cause a denial of service (invalid write operation and VMX process crash) or possibly execute arbitrary code on the host OS by leveraging administrative privileges on the guest OS.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	53369
CVE	CVE-2012-2450
DISA_SEVERITY	Category I
DISA_VMSKEY	V0032167
DISA_VMSKEY	V0032171
IAVM	2012-A-0072
IAVM	2012-A-0073
OSVDB	81695
OVAL	16852
URL	http://www.vmware.com/security/advisories/VMSA-2012-0009.html
XF	75377

Vulnerability Solution:

VMware Workstation >= 7 and < 7.1.6
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.1.60. VMware Player: Vulnerability (VMSA-2012-0011) (CVE-2012-3288) (vmsa-2012-0011-cve-2012-3288-player)

Description:

VMware Workstation 7.x before 7.1.6 and 8.x before 8.0.4, VMware Player 3.x before 3.1.6 and 4.x before 4.0.4, VMware Fusion 4.x before 4.1.3, VMware ESXi 3.5 through 5.0, and VMware ESX 3.5 through 4.1 allow user-assisted remote attackers to execute arbitrary code on the host OS or cause a denial of service (memory corruption) on the host OS via a crafted Checkpoint file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
CVE	CVE-2012-3288
DISA_SEVERITY	Category I
DISA_VMSKEY	V0032846
DISA_VMSKEY	V0032847
IAVM	2012-A-0099
IAVM	2012-A-0100
OVAL	17178
URL	http://www.vmware.com/security/advisories/VMSA-2012-0011.html

Vulnerability Solution:

•VMware Player >= 3.1 and < 3.1.6

Upgrade to VMware Player version 3.1.6

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 4.0 and < 4.0.4

Upgrade to VMware Player version 4.0.4

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.61. VMware Workstation: Vulnerability (VMSA-2012-0011) (CVE-2012-3288) (vmsa-2012-0011-cve-2012-3288-workstation)

Description:

VMware Workstation 7.x before 7.1.6 and 8.x before 8.0.4, VMware Player 3.x before 3.1.6 and 4.x before 4.0.4, VMware Fusion 4.x before 4.1.3, VMware ESXi 3.5 through 5.0, and VMware ESX 3.5 through 4.1 allow user-assisted remote attackers to execute arbitrary code on the host OS or cause a denial of service (memory corruption) on the host OS via a crafted Checkpoint file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
CVE	CVE-2012-3288
DISA_SEVERITY	Category I
DISA_VMSKEY	V0032846
DISA_VMSKEY	V0032847
IAVM	2012-A-0099
IAVM	2012-A-0100
OVAL	17178
URL	http://www.vmware.com/security/advisories/VMSA-2012-0011.html

Vulnerability Solution:

•VMware Workstation >= 7 and < 7.1.6

Upgrade to VMware Workstation version 7.1.6

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

•VMware Workstation >= 8 and < 8.0.4

Upgrade to VMware Workstation version 8.0.4

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/8_0

3.1.62. Apache HTTPD: APR-util XML DoS (CVE-2009-1955) (apache-httpd-cve-2009-1955)

Description:

The affected asset is vulnerable to this vulnerability ONLY if an attacker could convince Apache to consume a specially crafted XML document. Review your web server configuration for validation. A denial of service flaw was found in the bundled copy of the APR-util library Extensible Markup Language (XML) parser. A remote attacker could create a specially-crafted XML document that would cause excessive memory consumption when processed by the XML decoding engine.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2009-11-09-1
BID	35253
CVE	CVE-2009-1955
DEBIAN	DSA-1812
OVAL	10270
OVAL	12473
REDHAT	RHSA-2009:1107
REDHAT	RHSA-2009:1108
URL	http://httpd.apache.org/security/vulnerabilities_22.html

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.

3.1.63. Apache HTTPD: mod_proxy_ftp FTP command injection (CVE-2009-3095) (apache-httpd-cve-2009-3095)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy_ftp. Review your web server configuration for validation. A flaw was found in the mod_proxy_ftp module. In a reverse proxy configuration, a remote attacker could use this flaw to bypass intended access restrictions by creating a carefully-crafted HTTP Authorization header, allowing the attacker to send arbitrary commands to the FTP server.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2010-03-29-1
CVE	CVE-2009-3095
DEBIAN	DSA-1934

Source	Reference
OVAL	8662
OVAL	9363
SUSE	SUSE-SA:2009:050
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.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 < 2.2.14

Upgrade to Apache HTTPD version 2.2.14

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.14.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.

3.1.64. 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:
192.168.234.131:80	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

Source	Reference
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.

3.1.65. 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:
192.168.234.131:80	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.

3.1.66. 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:
192.168.234.131:80	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.

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

Description:

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

•/examples/jsp/num/numguess.jsp
•/examples/jsp/dates/date.jsp
•/examples/jsp/snp/snoop.jsp
•/examples/jsp/error/error.html
•/examples/jsp/sessions/carts.html
•/examples/jsp/checkbox/check.html
•/examples/jsp/colors/colors.html
•/examples/jsp/cal/login.html
•/examples/jsp/include/include.jsp
•/examples/jsp/forward/forward.jsp
•/examples/jsp/plugin/plugin.jsp
•/examples/jsp/jsptoserv/jsptoservlet.jsp
•/examples/jsp/simpletag/foo.jsp
•/examples/jsp/mail/sendmail.jsp
•/examples/servlet/HelloWorldExample
•/examples/servlet/RequestInfoExample
•/examples/servlet/RequestHeaderExample
•/examples/servlet/RequestParamExample
•/examples/servlet/CookieExample
•/examples/servlet/JndiServlet
•/examples/servlet/SessionExample
•/tomcat-docs/appdev/sample/web/hello.jsp

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:8180	Running HTTP serviceProduct Tomcat exists -- Apache TomcatHTTP GET request to http://192.168.234.131:8180/tomcat-docs/appdev/sample/web/hello.jsp

Affected Nodes:	Additional Information:
	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.

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

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:5900	Running VNC service

References:
None

Vulnerability Solution:
Remove or disable this service. If it is necessary, be sure to use well thought out (hard to crack) passwords. It is important to note that VNC truncates passwords to 8 bytes when authenticating, making it more susceptible to brute force attacks.
To protect data from eaves-droppers, tunneling VNC through SSH is recommended.
Additionally, restricting access to specific IP addresses using TCP wrappers is also recommended.
For more information on VNC, visit the VNC website.

3.1.69. CIFS NULL Session Permitted (cifs-nt-0001)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Found user(s) via named pipes.Found server name via named pipes.Found local group(s) via named pipes.Found policy for domain(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.

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

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:139	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian
192.168.234.131:445	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.

3.1.71. Samba receive_smb_raw() Buffer Overflow (cifs-samba-receive-smb-raw-bof)

Description:

Heap-based buffer overflow in the receive_smb_raw function in util/sock.c in Samba 3.0.0 through 3.0.29 allows remote attackers to execute arbitrary code via a crafted SMB response.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:139	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian
192.168.234.131:445	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-2008-06-30
BID	29404
BID	31255
CVE	CVE-2008-1105
DEBIAN	DSA-1590
OVAL	10020

Source	Reference
OVAL	5733
REDHAT	RHSA-2008:0288
REDHAT	RHSA-2008:0289
REDHAT	RHSA-2008:0290
SUSE	SUSE-SA:2008:026
URL	http://www.samba.org/samba/security/CVE-2008-1105.html
XF	42664
XF	45251

Vulnerability Solution:

Samba < 3.0.30
Download and apply the upgrade from: https://ftp.samba.org/pub/samba/stable/samba-3.0.30.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.

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

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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

Source	Reference
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.

3.1.73. ISC BIND: Specially crafted DNS data can cause a lockup in named (CVE-2012-5166) (dns-bind-cve-2012-5166)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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	55852
CVE	CVE-2012-5166
DEBIAN	DSA-2560

Source	Reference
OVAL	19706
REDHAT	RHSA-2012:1363
REDHAT	RHSA-2012:1364
REDHAT	RHSA-2012:1365
URL	https://kb.isc.org/article/AA-00801/0
URL	https://kb.isc.org/article/AA-00801/74/CVE-2012-5166%3A-Specially-crafted-DNS-data-can-cause-a-lockup-in-named.html

Vulnerability Solution:

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

3.1.74. ISC BIND: A Defect in Delegation Handling Can Be Exploited to Crash BIND (CVE-2014-8500) (dns-bind-cve-2014-8500)

Description:

ISC BIND 9.0.x through 9.8.x, 9.9.0 through 9.9.6, and 9.10.0 through 9.10.1 does not limit delegation chaining, which allows remote attackers to cause a denial of service (memory consumption and named crash) via a large or infinite number of referrals.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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-2015-09-16-4
BID	71590
CERT-VN	264212
CVE	CVE-2014-8500
DEBIAN	DSA-3094
NETBSD	NetBSD-SA2015-002
REDHAT	RHSA-2016:0078
URL	https://kb.isc.org/article/AA-01216/0

Vulnerability Solution:

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

3.1.75. ISC BIND: An error in handling TKEY queries can cause named to exit with a REQUIRE assertion failure (CVE-2015-5477) (dns-bind-cve-2015-5477)

Description:

named in ISC BIND 9.x before 9.9.7-P2 and 9.10.x before 9.10.2-P3 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via TKEY queries.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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	76092
CVE	CVE-2015-5477
DEBIAN	DSA-3319
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061291
IAVM	2015-B-0099
REDHAT	RHSA-2015:1513
REDHAT	RHSA-2015:1514
REDHAT	RHSA-2015:1515
REDHAT	RHSA-2016:0078
REDHAT	RHSA-2016:0079
URL	https://kb.isc.org/article/AA-01272/0

Vulnerability Solution:

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

3.1.76. ISC BIND: Parsing malformed keys may cause BIND to exit due to a failed assertion in buffer.c (CVE-2015-5722) (dns-bind-cve-2015-5722)

Description:

buffer.c in named in ISC BIND 9.x before 9.9.7-P3 and 9.10.x before 9.10.2-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) by creating a zone containing a malformed DNSSEC key and issuing a query for a name in that zone.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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-2015-10-21-8
BID	76605
CVE	CVE-2015-5722
DEBIAN	DSA-3350
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061377
IAVM	2015-A-0208
REDHAT	RHSA-2015:1705
REDHAT	RHSA-2015:1706
REDHAT	RHSA-2015:1707
REDHAT	RHSA-2016:0078
REDHAT	RHSA-2016:0079
URL	https://kb.isc.org/article/AA-01287/0

Vulnerability Solution:

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

3.1.77. ISC BIND: Assertion Failure in buffer.c While Building Responses to a Specifically Constructed Request (CVE-2016-2776) (dns-bind-cve-2016-2776)

Description:

buffer.c in named in ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 does not properly construct responses, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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	93188
CVE	CVE-2016-2776
DISA_SEVERITY	Category I
IAVM	2017-A-0004
REDHAT	RHSA-2016:1944
REDHAT	RHSA-2016:1945
REDHAT	RHSA-2016:2099
URL	https://kb.isc.org/article/AA-01419/0

Vulnerability Solution:

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

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

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
CVE	CVE-2009-3291
CVE	CVE-2009-3292
CVE	CVE-2009-3293
DEBIAN	DSA-1940
OVAL	10438
OVAL	7047
OVAL	7394
OVAL	7652
OVAL	9982
URL	http://bugs.php.net/44683
URL	http://www.php.net/ChangeLog-5.php#5.2.11
URL	http://www.php.net/releases/5_2_11.php
XF	53334

Vulnerability Solution:

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

3.1.79. PHP Upgraded PCRE to version 7.8 (http-php-multiple-vulns-5-2-7)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2008-10-09
APPLE	APPLE-SA-2009-05-12

Source	Reference
BID	30087
BID	31681
CERT	TA09-133A
CVE	CVE-2008-2371
DEBIAN	DSA-1602

Vulnerability Solution:

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

3.1.80. PHP Multiple Vulnerabilities Fixed in version 5.3.1 (http-php-multiple-vulns-5-3-1)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
APPLE	APPLE-SA-2010-03-29-1
CVE	CVE-2009-3292
CVE	CVE-2009-3557
CVE	CVE-2009-3558
CVE	CVE-2009-3559
CVE	CVE-2009-4017
DEBIAN	DSA-1940
OVAL	10483
OVAL	6667
OVAL	7396
OVAL	7652

Source	Reference
OVAL	9982
URL	http://www.php.net/ChangeLog-5.php#5.3.1
URL	http://www.php.net/releases/5_3_1.php
XF	54455

Vulnerability Solution:

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

3.1.81. MySQL default account: root/no password (mysql-default-account-root-nopassword)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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.

3.1.82. MySQL yaSSL CertDecoder::GetName Multiple Buffer Overflows (mysql-yassl-certdecodergetname-multiple-bofs)

Description:

Multiple stack-based buffer overflows in the CertDecoder::GetName function in src/asn.cpp in TaoCrypt in yaSSL before 1.9.9, as used in mysqld in MySQL 5.0.x before 5.0.90, MySQL 5.1.x before 5.1.43, MySQL 5.5.x through 5.5.0-m2, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption and daemon crash) by establishing an SSL

connection and sending an X.509 client certificate with a crafted name field, as demonstrated by mysql_overflow1.py and the vd_mysql5 module in VulnDisco Pack Professional 8.11. NOTE: this was originally reported for MySQL 5.0.51a.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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	37640
BID	37943
BID	37974
CVE	CVE-2009-4484
DEBIAN	DSA-1997
URL	http://bugs.mysql.com/bug.php?id=50227
URL	http://dev.mysql.com/doc/refman/5.0/en/news-5-0-90.html
URL	http://dev.mysql.com/doc/refman/5.1/en/news-5-1-43.html
XF	55416

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.90

Upgrade to Oracle MySQL version 5.0.90

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 < 5.1.43

Upgrade to Oracle MySQL version 5.1.43

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.

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

Description:

A weakness has been discovered in the random number generator used by OpenSSL on Debian and Ubuntu systems. As a result of this weakness, certain encryption keys are much more common than they should be, such that an attacker could guess the key through

a brute-force attack given minimal knowledge of the system. This particularly affects the use of encryption keys in OpenSSH, OpenVPN and SSL certificates. This vulnerability only affects operating systems which are based on Debian. However, other systems can be indirectly affected if weak keys are imported into them.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:22	SSH public key with fingerprint 5656240F211DDEA72BAE61B1243DE8F3 is a known weak key

References:

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

3.1.84. PHP crash inside gd with invalid fonts (php-crash-inside-gd-with-invalid-fonts)

Description:

Buffer overflow in the imageloadfont function in ext/gd/gd.c in PHP 4.4.x before 4.4.9 and PHP 5.2 before 5.2.6-r6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	30649
CERT	TA09-133A
CVE	CVE-2008-3658
DEBIAN	DSA-1647
OVAL	9724
REDHAT	RHSA-2009:0350
XF	44401

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

3.1.85. PHP Vulnerability: CVE-2008-2107 (php-cve-2008-2107)

Description:

The GENERATE_SEED macro in PHP 4.x before 4.4.8 and 5.x before 5.2.5, when running on 32-bit systems, performs a multiplication using values that can produce a zero seed in rare circumstances, which allows context-dependent attackers to predict subsequent values of the rand and mt_rand functions and possibly bypass protection mechanisms that rely on an unknown initial seed.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2008-2107
DEBIAN	DSA-1789
OVAL	10644
REDHAT	RHSA-2008:0505
REDHAT	RHSA-2008:0544
REDHAT	RHSA-2008:0545
REDHAT	RHSA-2008:0546
REDHAT	RHSA-2008:0582
XF	42226
XF	42284

Vulnerability Solution:

•Upgrade to PHP version 4.4.8

Download and apply the upgrade from: http://museum.php.net/php4/php-4.4.8.tar.gz

•Upgrade to PHP version 5.2.5

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

3.1.86. PHP Vulnerability: CVE-2008-2108 (php-cve-2008-2108)

Description:

The GENERATE_SEED macro in PHP 4.x before 4.4.8 and 5.x before 5.2.5, when running on 64-bit systems, performs a multiplication that generates a portion of zero bits during conversion due to insufficient precision, which produces 24 bits of entropy and simplifies brute force attacks against protection mechanisms that use the rand and mt_rand functions.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2008-2108
DEBIAN	DSA-1789
OVAL	10844
REDHAT	RHSA-2008:0505
REDHAT	RHSA-2008:0544
REDHAT	RHSA-2008:0545
REDHAT	RHSA-2008:0546
REDHAT	RHSA-2008:0582
XF	42226

Vulnerability Solution:

•Upgrade to PHP version 4.4.8

Download and apply the upgrade from: http://museum.php.net/php4/php-4.4.8.tar.gz

•Upgrade to PHP version 5.2.5

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

3.1.87. PHP Vulnerability: CVE-2008-3658 (php-cve-2008-3658)

Description:

Buffer overflow in the imageloadfont function in ext/gd/gd.c in PHP 4.4.x before 4.4.9 and PHP 5.2 before 5.2.6-r6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-05-12

Source	Reference
BID	30649
CERT	TA09-133A
CVE	CVE-2008-3658
DEBIAN	DSA-1647
OVAL	9724
REDHAT	RHSA-2009:0350
XF	44401

Vulnerability Solution:

•Upgrade to PHP version 4.4.9

Download and apply the upgrade from: http://museum.php.net/php4/php-4.4.9.tar.gz

•Upgrade to PHP version 5.2.6

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

3.1.88. PHP Vulnerability: CVE-2008-5624 (php-cve-2008-5624)

Description:

PHP 5 before 5.2.7 does not properly initialize the page_uid and page_gid global variables for use by the SAPI php_getuid function, which allows context-dependent attackers to bypass safe_mode restrictions via variable settings that are intended to be restricted to root, as demonstrated by a setting of /etc for the error_log variable.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	32688
CVE	CVE-2008-5624
DEBIAN	DSA-1789
XF	47318

Vulnerability Solution:

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

3.1.89. PHP Vulnerability: CVE-2008-5625 (php-cve-2008-5625)

Description:

PHP 5 before 5.2.7 does not enforce the error_log safe_mode restrictions when safe_mode is enabled through a php_admin_flag setting in httpd.conf, which allows context-dependent attackers to write to arbitrary files by placing a "php_value error_log" entry in a .htaccess file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	32383
CVE	CVE-2008-5625
XF	47314

Vulnerability Solution:

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

3.1.90. PHP Vulnerability: CVE-2008-5658 (php-cve-2008-5658)

Description:

Directory traversal vulnerability in the ZipArchive::extractTo function in PHP 5.2.6 and earlier allows context-dependent attackers to write arbitrary files via a ZIP file with a file whose name contains .. (dot dot) sequences.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	32625
CVE	CVE-2008-5658
DEBIAN	DSA-1789
REDHAT	RHSA-2009:0350

Source	Reference
XF	47079

Vulnerability Solution:

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

3.1.91. PHP Vulnerability: CVE-2009-3291 (php-cve-2009-3291)

Description:

The php_openssl_apply_verification_policy function in PHP before 5.2.11 does not properly perform certificate validation, which has unknown impact and attack vectors, probably related to an ability to spoof certificates.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
CVE	CVE-2009-3291
DEBIAN	DSA-1940
OVAL	10438
OVAL	7394
URL	http://www.php.net/ChangeLog-5.php#5.2.11
URL	http://www.php.net/releases/5_2_11.php
XF	53334

Vulnerability Solution:

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

3.1.92. PHP Vulnerability: CVE-2009-3292 (php-cve-2009-3292)

Description:

Unspecified vulnerability in PHP before 5.2.11, and 5.3.x before 5.3.1, has unknown impact and attack vectors related to "missing sanity checks around exif processing."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
CVE	CVE-2009-3292
DEBIAN	DSA-1940
OVAL	7652
OVAL	9982
URL	http://www.php.net/ChangeLog-5.php#5.2.11

Vulnerability Solution:

•Upgrade to PHP version 5.2.11

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

•Upgrade to PHP version 5.3.1

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

3.1.93. PHP Vulnerability: CVE-2009-3293 (php-cve-2009-3293)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
CVE	CVE-2009-3293
OVAL	7047
URL	http://www.php.net/ChangeLog-5.php#5.2.11

Source	Reference
URL	http://www.php.net/releases/5_2_11.php

Vulnerability Solution:

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

3.1.94. PHP Vulnerability: CVE-2009-4018 (php-cve-2009-4018)

Description:

The proc_open function in ext/standard/proc_open.c in PHP before 5.2.11 and 5.3.x before 5.3.1 does not enforce the (1) safe_mode_allowed_env_vars and (2) safe_mode_protected_env_vars directives, which allows context-dependent attackers to execute programs with an arbitrary environment via the env parameter, as demonstrated by a crafted value of the LD_LIBRARY_PATH environment variable.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	37138
CVE	CVE-2009-4018
OVAL	7256

Vulnerability Solution:

•Upgrade to PHP version 5.2.11

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

•Upgrade to PHP version 5.3.1

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

3.1.95. PHP Vulnerability: CVE-2010-1129 (php-cve-2010-1129)

Description:

The safe_mode implementation in PHP before 5.2.13 does not properly handle directory pathnames that lack a trailing / (slash) character, which allows context-dependent attackers to bypass intended access restrictions via vectors related to use of the tempnam function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2010-08-24-1
BID	38431
CVE	CVE-2010-1129

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.13.tar.gz

3.1.96. PHP Vulnerability: CVE-2014-3669 (php-cve-2014-3669)

Description:

Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
BID	70611
CVE	CVE-2014-3669
DEBIAN	DSA-3064
REDHAT	RHSA-2014:1765
REDHAT	RHSA-2014:1766
REDHAT	RHSA-2014:1767
REDHAT	RHSA-2014:1768
REDHAT	RHSA-2014:1824

Source	Reference
URL	https://bugs.php.net/bug.php?id=68044

Vulnerability Solution:

•Upgrade to PHP version 5.4.34

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

•Upgrade to PHP version 5.5.18

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

•Upgrade to PHP version 5.6.2

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

3.1.97. PHP Vulnerability: CVE-2014-9912 (php-cve-2014-9912)

Description:

The get_icu_disp_value_src_php function in ext/intl/locale/locale_methods.c in PHP before 5.3.29, 5.4.x before 5.4.30, and 5.5.x before 5.5.14 does not properly restrict calls to the ICU uresbund.cpp component, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a locale_get_display_name call with a long first argument.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	68549
CVE	CVE-2014-9912
URL	http://www.php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=67397

Vulnerability Solution:

•Upgrade to PHP version 5.3.29

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

•Upgrade to PHP version 5.4.30

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

•Upgrade to PHP version 5.5.14

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

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

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2015-08-13-2
APPLE	APPLE-SA-2015-09-30-3
BID	73431
CVE	CVE-2015-2787
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061337
IAVM	2015-A-0199
REDHAT	RHSA-2015:1053
REDHAT	RHSA-2015:1066
REDHAT	RHSA-2015:1135
REDHAT	RHSA-2015:1218

Vulnerability Solution:

•Upgrade to PHP version 5.4.39

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

•Upgrade to PHP version 5.5.23

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

•Upgrade to PHP version 5.6.7

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

3.1.99. PHP Vulnerability: CVE-2015-4022 (php-cve-2015-4022)

Description:

Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2015-08-13-2
BID	74902
CVE	CVE-2015-4022
DEBIAN	DSA-3280
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061337
IAVM	2015-A-0199
REDHAT	RHSA-2015:1135
REDHAT	RHSA-2015:1186
REDHAT	RHSA-2015:1187
REDHAT	RHSA-2015:1218
REDHAT	RHSA-2015:1219
URL	https://bugs.php.net/bug.php?id=69545

Vulnerability Solution:

•Upgrade to PHP version 5.4.41

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

•Upgrade to PHP version 5.5.25

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

•Upgrade to PHP version 5.6.9

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

3.1.100. PHP Vulnerability: CVE-2015-4026 (php-cve-2015-4026)

Description:

The pcntl_exec implementation in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \x00 character, which might allow remote attackers to bypass intended extension restrictions and execute files with unexpected names via a crafted first argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2015-08-13-2
BID	75056
CVE	CVE-2015-4026
DEBIAN	DSA-3280
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061337
IAVM	2015-A-0199
REDHAT	RHSA-2015:1135
REDHAT	RHSA-2015:1186
REDHAT	RHSA-2015:1187
REDHAT	RHSA-2015:1218
REDHAT	RHSA-2015:1219

Vulnerability Solution:

•Upgrade to PHP version 5.4.41

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

•Upgrade to PHP version 5.5.25

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

•Upgrade to PHP version 5.6.9

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

3.1.101. PHP Vulnerability: CVE-2015-4147 (php-cve-2015-4147)

Description:

The SoapClient::__call method in ext/soap/soap.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 does not verify that __default_headers is an array, which allows remote attackers to execute arbitrary code by providing crafted serialized data with an unexpected data type, related to a "type confusion" issue.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2015-08-13-2
BID	73357
CVE	CVE-2015-4147
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061337
IAVM	2015-A-0199
REDHAT	RHSA-2015:1053
REDHAT	RHSA-2015:1066
REDHAT	RHSA-2015:1135
REDHAT	RHSA-2015:1218

Vulnerability Solution:

•Upgrade to PHP version 5.4.39

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

•Upgrade to PHP version 5.5.23

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

•Upgrade to PHP version 5.6.7

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

3.1.102. PHP Vulnerability: CVE-2015-4598 (php-cve-2015-4598)

Description:

PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read or write to arbitrary files via crafted input to an application that calls (1) a DOMDocument save method or (2) the GD imagepsloadfont function, as demonstrated by a filename\0.html attack that bypasses an intended configuration in which client users may write to only .html files.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	75244
CVE	CVE-2015-4598
DEBIAN	DSA-3344
REDHAT	RHSA-2015:1135
REDHAT	RHSA-2015:1186
REDHAT	RHSA-2015:1187
REDHAT	RHSA-2015:1218
REDHAT	RHSA-2015:1219

Vulnerability Solution:

•Upgrade to PHP version 5.4.42

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

•Upgrade to PHP version 5.5.26

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

•Upgrade to PHP version 5.6.10

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

3.1.103. PHP Vulnerability: CVE-2015-4643 (php-cve-2015-4643)

Description:

Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-4022.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	75291
CVE	CVE-2015-4643
DEBIAN	DSA-3344
REDHAT	RHSA-2015:1135

Source	Reference
REDHAT	RHSA-2015:1186
REDHAT	RHSA-2015:1187
REDHAT	RHSA-2015:1218

Vulnerability Solution:

•Upgrade to PHP version 5.4.42

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

•Upgrade to PHP version 5.5.26

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

•Upgrade to PHP version 5.6.10

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

3.1.104. PHP Vulnerability: CVE-2015-5590 (php-cve-2015-5590)

Description:

Stack-based buffer overflow in the phar_fix_filepath function in ext/phar/phar.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large length value, as demonstrated by mishandling of an e-mail attachment by the imap PHP extension.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	75970
CVE	CVE-2015-5590
DEBIAN	DSA-3344
URL	http://www.php.net/ChangeLog-5.php

Vulnerability Solution:

•Upgrade to PHP version 5.4.43

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

•Upgrade to PHP version 5.5.27

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

•Upgrade to PHP version 5.6.11

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

3.1.105. PHP Vulnerability: CVE-2015-6831 (php-cve-2015-6831)

Description:

Multiple use-after-free vulnerabilities in SPL in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allow remote attackers to execute arbitrary code via vectors involving (1) ArrayObject, (2) SplObjectStorage, and (3) SplDoublyLinkedList, which are mishandled during unserialization.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	76737
CVE	CVE-2015-6831
DEBIAN	DSA-3344
URL	http://www.php.net/ChangeLog-5.php

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/

3.1.106. PHP Vulnerability: CVE-2015-6832 (php-cve-2015-6832)

Description:

Use-after-free vulnerability in the SPL unserialize implementation in ext/spl/spl_array.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to execute arbitrary code via crafted serialized data that triggers misuse of an array field.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2015-6832
DEBIAN	DSA-3344
URL	http://www.php.net/ChangeLog-5.php

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/

3.1.107. PHP Vulnerability: CVE-2015-6836 (php-cve-2015-6836)

Description:

The SoapClient __call method in ext/soap/soap.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 does not properly manage headers, which allows remote attackers to execute arbitrary code via crafted serialized data that triggers a "type confusion" in the serialize_function_call function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	76644
CVE	CVE-2015-6836
DEBIAN	DSA-3358
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061365
IAVM	2015-B-0108
URL	http://www.php.net/ChangeLog-5.php

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/

3.1.108. PHP Vulnerability: CVE-2015-8835 (php-cve-2015-8835)

Description:

The make_http_soap_request function in ext/soap/php_http.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 does not properly retrieve keys, which allows remote attackers to cause a denial of service (NULL pointer dereference, type confusion, and application crash) or possibly execute arbitrary code via crafted serialized data representing a numerically indexed _cookies array, related to the SoapClient::__call method in ext/soap/soap.c.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	84426
CVE	CVE-2015-8835
REDHAT	RHSA-2016:2750

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/

3.1.109. PHP Vulnerability: CVE-2015-8865 (php-cve-2015-8865)

Description:

The file_check_mem function in funcs.c in file before 5.23, as used in the Fileinfo component in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5, mishandles continuation-level jumps, which allows context-dependent attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code via a crafted magic file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2016-05-16-4
BID	85802
CVE	CVE-2015-8865
DEBIAN	DSA-3560
REDHAT	RHSA-2016:2750

Vulnerability Solution:

•Upgrade to PHP version 5.5.34

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

•Upgrade to PHP version 5.6.20

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

•Upgrade to PHP version 7.0.5

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

3.1.110. PHP Vulnerability: CVE-2016-4073 (php-cve-2016-4073)

Description:

Multiple integer overflows in the mbfl_strcut function in ext/mbstring/libmbfl/mbfl/mbfilter.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted mb_strcut call.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2016-05-16-4

Source	Reference
BID	85991
CVE	CVE-2016-4073
DEBIAN	DSA-3560
REDHAT	RHSA-2016:2750

Vulnerability Solution:

•Upgrade to PHP version 5.5.34

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

•Upgrade to PHP version 5.6.20

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

•Upgrade to PHP version 7.0.5

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

3.1.111. PHP Vulnerability: CVE-2016-4537 (php-cve-2016-4537)

Description:

The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 accepts a negative integer for the scale argument, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	90173
CVE	CVE-2016-4537
DEBIAN	DSA-3602
DISA_SEVERITY	Category I
IAVM	2016-B-0160
REDHAT	RHSA-2016:2750

Vulnerability Solution:

•Upgrade to PHP version 5.5.35

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

•Upgrade to PHP version 5.6.21

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

•Upgrade to PHP version 7.0.6

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

3.1.112. PHP Vulnerability: CVE-2016-4538 (php-cve-2016-4538)

Description:

The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 modifies certain data structures without considering whether they are copies of the _zero_, _one_, or _two_ global variable, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	90173
CVE	CVE-2016-4538
DEBIAN	DSA-3602
DISA_SEVERITY	Category I
IAVM	2016-B-0160
REDHAT	RHSA-2016:2750

Vulnerability Solution:

•Upgrade to PHP version 5.5.35

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

•Upgrade to PHP version 5.6.21

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

•Upgrade to PHP version 7.0.6

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

3.1.113. PHP Vulnerability: CVE-2016-4539 (php-cve-2016-4539)

Description:

The xml_parse_into_struct function in ext/xml/xml.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (buffer under-read and segmentation fault) or possibly have unspecified other impact via crafted

XML data in the second argument, leading to a parser level of zero.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	90174
CVE	CVE-2016-4539
DEBIAN	DSA-3602
DISA_SEVERITY	Category I
IAVM	2016-B-0160
REDHAT	RHSA-2016:2750

Vulnerability Solution:

•Upgrade to PHP version 5.5.35

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

•Upgrade to PHP version 5.6.21

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

•Upgrade to PHP version 7.0.6

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

3.1.114. PHP Vulnerability: CVE-2016-4542 (php-cve-2016-4542)

Description:

The exif_process_IFD_TAG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not properly construct spprintf arguments, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	89844
CVE	CVE-2016-4542
DEBIAN	DSA-3602
DISA_SEVERITY	Category I
IAVM	2016-B-0160
REDHAT	RHSA-2016:2750

Vulnerability Solution:

•Upgrade to PHP version 5.5.35

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

•Upgrade to PHP version 5.6.21

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

•Upgrade to PHP version 7.0.6

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

3.1.115. PHP Vulnerability: CVE-2016-4543 (php-cve-2016-4543)

Description:

The exif_process_IFD_in_JPEG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not validate IFD sizes, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	89844
CVE	CVE-2016-4543
DEBIAN	DSA-3602
DISA_SEVERITY	Category I
IAVM	2016-B-0160
REDHAT	RHSA-2016:2750

Vulnerability Solution:

•Upgrade to PHP version 5.5.35

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

•Upgrade to PHP version 5.6.21

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

•Upgrade to PHP version 7.0.6

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

3.1.116. PHP Vulnerability: CVE-2016-4544 (php-cve-2016-4544)

Description:

The exif_process_TIFF_in_JPEG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not validate TIFF start data, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	89844
CVE	CVE-2016-4544
DEBIAN	DSA-3602
REDHAT	RHSA-2016:2750

Vulnerability Solution:

•Upgrade to PHP version 5.5.35

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

•Upgrade to PHP version 5.6.21

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

•Upgrade to PHP version 7.0.6

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

3.1.117. PHP Vulnerability: CVE-2016-5096 (php-cve-2016-5096)

Description:

Integer overflow in the fread function in ext/standard/file.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large integer in the second argument.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	90861
CVE	CVE-2016-5096
DEBIAN	DSA-3602
REDHAT	RHSA-2016:2750

Vulnerability Solution:

•Upgrade to PHP version 5.5.36

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

•Upgrade to PHP version 5.6.22

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

3.1.118. PHP Vulnerability: CVE-2016-5768 (php-cve-2016-5768)

Description:

Double free vulnerability in the _php_mb_regex_ereg_replace_exec function in php_mbregex.c in the mbstring extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) by leveraging a callback exception.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2016-09-20
BID	91396

Source	Reference
CVE	CVE-2016-5768
DEBIAN	DSA-3618
REDHAT	RHSA-2016:2598
REDHAT	RHSA-2016:2750
URL	https://bugs.php.net/bug.php?id=72402

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/

•Upgrade to PHP version 7.0.8

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

3.1.119. PHP Vulnerability: CVE-2016-5771 (php-cve-2016-5771)

Description:

spl_array.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2016-09-20
BID	91401
CVE	CVE-2016-5771
DEBIAN	DSA-3618
REDHAT	RHSA-2016:2750
URL	https://bugs.php.net/bug.php?id=72433

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/

3.1.120. PHP Vulnerability: CVE-2016-5772 (php-cve-2016-5772)

Description:

Double free vulnerability in the php_wddx_process_data function in wddx.c in the WDDX extension 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 (application crash) or possibly execute arbitrary code via crafted XML data that is mishandled in a wddx_deserialize call.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2016-09-20
BID	91398
CVE	CVE-2016-5772
DEBIAN	DSA-3618
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/

•Upgrade to PHP version 7.0.8

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

3.1.121. PHP Vulnerability: CVE-2016-6288 (php-cve-2016-6288)

Description:

The php_url_parse_ex function in ext/standard/url.c in PHP before 5.5.38 allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via vectors involving the smart_str data type.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2016-09-20
BID	92111
CVE	CVE-2016-6288
REDHAT	RHSA-2016:2750
URL	https://bugs.php.net/70480

Vulnerability Solution:

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

3.1.122. PHP Vulnerability: CVE-2016-6290 (php-cve-2016-6290)

Description:

ext/session/session.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly maintain a certain hash data structure, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to session deserialization.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2016-09-20
BID	92097
CVE	CVE-2016-6290
DEBIAN	DSA-3631
REDHAT	RHSA-2016:2750

Vulnerability Solution:

•Upgrade to PHP version 5.5.38
Download and apply the upgrade from: http://www.php.net/releases/
•Upgrade to PHP version 5.6.24
Download and apply the upgrade from: http://www.php.net/releases/
•Upgrade to PHP version 7.0.9
Download and apply the upgrade from: http://www.php.net/releases/

3.1.123. PHP Vulnerability: CVE-2016-6291 (php-cve-2016-6291)

Description:

The exif_process_IFD_in_MAKERNOTE function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds array access and memory corruption), obtain sensitive information from process memory, or possibly have unspecified other impact via a crafted JPEG image.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2016-09-20
BID	92073
CVE	CVE-2016-6291
DEBIAN	DSA-3631
REDHAT	RHSA-2016:2750
URL	https://bugs.php.net/72603

Vulnerability Solution:

•Upgrade to PHP version 5.5.38
Download and apply the upgrade from: http://www.php.net/releases/
•Upgrade to PHP version 5.6.24
Download and apply the upgrade from: http://www.php.net/releases/
•Upgrade to PHP version 7.0.9
Download and apply the upgrade from: http://www.php.net/releases/

3.1.124. PHP Vulnerability: CVE-2016-6296 (php-cve-2016-6296)

Description:

Integer signedness error in the simplestring_addn function in simplestring.c in xmlrpc-epi through 0.54.2, as used in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a long first argument to the PHP xmlrpc_encode_request function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2016-09-20
BID	92095
CVE	CVE-2016-6296
DEBIAN	DSA-3631
REDHAT	RHSA-2016:2750

Vulnerability Solution:

•Upgrade to PHP version 5.5.38

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

•Upgrade to PHP version 5.6.24

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

•Upgrade to PHP version 7.0.9

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

3.1.125. PHP Vulnerability: CVE-2016-7124 (php-cve-2016-7124)

Description:

ext/standard/var_unserializer.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles certain invalid objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that leads to a (1) __destruct call or (2) magic method call.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	92756
CVE	CVE-2016-7124
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/

3.1.126. 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:
192.168.234.131:80	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
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/

3.1.127. PHP Vulnerability: CVE-2016-7127 (php-cve-2016-7127)

Description:

The imagegammacorrect function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate gamma values, which allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by providing different signs for the second and third arguments.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	92757
CVE	CVE-2016-7127
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/

3.1.128. PHP Vulnerability: CVE-2016-7129 (php-cve-2016-7129)

Description:

The php_wddx_process_data function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via an invalid ISO 8601 time value, as demonstrated by a wddx_deserialize call that mishandles a dateTime element in a wddxPacket XML document.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	92758

Source	Reference
CVE	CVE-2016-7129
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/

3.1.129. PHP Vulnerability: CVE-2016-7411 (php-cve-2016-7411)

Description:

ext/standard/var_unserializer.re in PHP before 5.6.26 mishandles object-deserialization failures, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via an unserialize call that references a partially constructed object.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	93009
CVE	CVE-2016-7411

Vulnerability Solution:

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

3.1.130. PHP Vulnerability: CVE-2016-7413 (php-cve-2016-7413)

Description:

Use-after-free vulnerability in the wddx_stack_destroy function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a wddxPacket XML document that lacks an end-tag for a recordset field element, leading to mishandling in a wddx_deserialize call.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	93006
CVE	CVE-2016-7413

Vulnerability Solution:

•Upgrade to PHP version 5.6.26

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

•Upgrade to PHP version 7.0.11

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

3.1.131. PHP Vulnerability: CVE-2016-7417 (php-cve-2016-7417)

Description:

ext/spl/spl_array.c in PHP before 5.6.26 and 7.x before 7.0.11 proceeds with SplArray unserialization without validating a return value and data type, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	93007
CVE	CVE-2016-7417

Vulnerability Solution:

•Upgrade to PHP version 5.6.26

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

•Upgrade to PHP version 7.0.11

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

3.1.132. PHP Vulnerability: CVE-2016-9137 (php-cve-2016-9137)

Description:

Use-after-free vulnerability in the CURLFile implementation in ext/curl/curl_file.c in PHP before 5.6.27 and 7.x before 7.0.12 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that is mishandled during __wakeup processing.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	93577
CVE	CVE-2016-9137
DEBIAN	DSA-3698
URL	http://www.php.net/ChangeLog-5.php
URL	http://www.php.net/ChangeLog-7.php
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/

3.1.133. 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:
192.168.234.131:80	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/

3.1.134. PHP Vulnerability: CVE-2016-9935 (php-cve-2016-9935)

Description:

The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.29 and 7.x before 7.0.14 allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) or possibly have unspecified other impact via an empty boolean element in a wddxPacket XML document.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	94846
CVE	CVE-2016-9935
DEBIAN	DSA-3737
URL	http://www.php.net/ChangeLog-5.php
URL	http://www.php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=73631

Vulnerability Solution:

•Upgrade to PHP version 5.6.29

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

•Upgrade to PHP version 7.0.14

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

3.1.135. PHP Vulnerability: CVE-2017-12933 (php-cve-2017-12933)

Description:

The finish_nested_data function in ext/standard/var_unserializer.re in PHP before 5.6.31, 7.0.x before 7.0.21, and 7.1.x before 7.1.7 is prone to a buffer over-read while unserializing untrusted data. Exploitation of this issue can have an unspecified impact on the integrity of PHP.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	99490
CVE	CVE-2017-12933
DEBIAN	DSA-4080
DEBIAN	DSA-4081
URL	https://bugs.php.net/bug.php?id=74111

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/

3.1.136. PHP Vulnerability: CVE-2018-7584 (php-cve-2018-7584)

Description:

In PHP through 5.6.33, 7.0.x before 7.0.28, 7.1.x through 7.1.14, and 7.2.x through 7.2.2, there is a stack-based buffer under-read while parsing an HTTP response in the php_stream_url_wrap_http_ex function in ext/standard/http_fopen_wrapper.c. This subsequently results in copying a large string.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.234.130:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.29 Vulnerable version of component PHP found -- PHP 7.2.1
192.168.234.130:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPD 2.4.29 Vulnerable version of component PHP found -- PHP 7.2.1
192.168.234.131:80	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	103204
CVE	CVE-2018-7584

Vulnerability Solution:

•Upgrade to PHP version 5.6.34

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

•Upgrade to PHP version 7.0.28

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

•Upgrade to PHP version 7.1.15

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

•Upgrade to PHP version 7.2.3

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

3.1.137. PHP Upgraded PCRE to version 7.8 (php-upgraded-pcre-to-version-7-8)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2008-10-09
APPLE	APPLE-SA-2009-05-12

Source	Reference
BID	30087
BID	31681
CERT	TA09-133A
CVE	CVE-2008-2371
DEBIAN	DSA-1602

Vulnerability Solution:

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

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

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:513	Running Remote Login service

References:

Source	Reference
CVE	CVE-1999-0651

Vulnerability Solution:

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

3.1.139. 'rsh' Remote Shell Service Enabled (service-rsh)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:514	Running Remote Shell service

References:

Source	Reference
CVE	CVE-1999-0651

Vulnerability Solution:

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

3.1.140. VMware Player: Updated OpenSSL library to address various security vulnerabilities (VMSA-2008-0005) (CVE-2006-2937) (vmsa-2008-0005-cve-2006-2937-player)

Description:

OpenSSL 0.9.7 before 0.9.7l and 0.9.8 before 0.9.8d allows remote attackers to cause a denial of service (infinite loop and memory consumption) via malformed ASN.1 structures that trigger an improperly handled error condition.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
APPLE	APPLE-SA-2006-11-28
BID	20248
BID	28276
CERT	TA06-333A
CERT-VN	247744
CVE	CVE-2006-2937
DEBIAN	DSA-1185
NETBSD	NetBSD-SA2008-007
OVAL	10560
REDHAT	RHSA-2006:0695
REDHAT	RHSA-2008:0629
SGI	20061001-01-P
SUSE	SUSE-SA:2006:058
URL	http://www.vmware.com/security/advisories/VMSA-2008-0005.html
XF	29228

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.6

Upgrade to VMware Player version 1.0.6

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.0 and < 2.0.3

Upgrade to VMware Player version 2.0.3

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.141. VMware Workstation: Updated OpenSSL library to address various security vulnerabilities (VMSA-2008-0005) (CVE-2006-2937) (vmsa-2008-0005-cve-2006-2937-workstation)

Description:

OpenSSL 0.9.7 before 0.9.7l and 0.9.8 before 0.9.8d allows remote attackers to cause a denial of service (infinite loop and memory consumption) via malformed ASN.1 structures that trigger an improperly handled error condition.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
APPLE	APPLE-SA-2006-11-28
BID	20248
BID	28276
CERT	TA06-333A
CERT-VN	247744
CVE	CVE-2006-2937
DEBIAN	DSA-1185
NETBSD	NetBSD-SA2008-007
OVAL	10560
REDHAT	RHSA-2006:0695
REDHAT	RHSA-2008:0629
SGI	20061001-01-P
SUSE	SUSE-SA:2006:058
URL	http://www.vmware.com/security/advisories/VMSA-2008-0005.html
XF	29228

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.6

Upgrade to VMware Workstation version 5.5.6

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6 and < 6.0.3

Upgrade to VMware Workstation version 6.0.3

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.1.142. VMware Player: Updated OpenSSL library to address various security vulnerabilities (VMSA-2008-0005) (CVE-2006-2940) (vmsa-2008-0005-cve-2006-2940-player)

Description:

OpenSSL 0.9.7 before 0.9.7l, 0.9.8 before 0.9.8d, and earlier versions allows attackers to cause a denial of service (CPU consumption) via parasitic public keys with large (1) "public exponent" or (2) "public modulus" values in X.509 certificates that require extra time to process when using RSA signature verification.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
APPLE	APPLE-SA-2006-11-28
BID	20247
BID	22083
BID	28276
CERT	TA06-333A
CVE	CVE-2006-2940
DEBIAN	DSA-1185
DEBIAN	DSA-1195
NETBSD	NetBSD-SA2008-007
OVAL	10311
REDHAT	RHSA-2006:0695
REDHAT	RHSA-2008:0629
SGI	20061001-01-P
SUSE	SUSE-SA:2006:058

Source	Reference
URL	http://www.vmware.com/security/advisories/VMSA-2008-0005.html
XF	29230

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.6

Upgrade to VMware Player version 1.0.6

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.0 and < 2.0.3

Upgrade to VMware Player version 2.0.3

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.143. VMware Workstation: Updated OpenSSL library to address various security vulnerabilities (VMSA-2008-0005) (CVE-2006-2940) (vmsa-2008-0005-cve-2006-2940-workstation)

Description:

OpenSSL 0.9.7 before 0.9.7l, 0.9.8 before 0.9.8d, and earlier versions allows attackers to cause a denial of service (CPU consumption) via parasitic public keys with large (1) "public exponent" or (2) "public modulus" values in X.509 certificates that require extra time to process when using RSA signature verification.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
APPLE	APPLE-SA-2006-11-28
BID	20247
BID	22083
BID	28276
CERT	TA06-333A
CVE	CVE-2006-2940
DEBIAN	DSA-1185
DEBIAN	DSA-1195
NETBSD	NetBSD-SA2008-007
OVAL	10311
REDHAT	RHSA-2006:0695

Source	Reference
REDHAT	RHSA-2008:0629
SGI	20061001-01-P
SUSE	SUSE-SA:2006:058
URL	http://www.vmware.com/security/advisories/VMSA-2008-0005.html
XF	29230

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.6

Upgrade to VMware Workstation version 5.5.6

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6 and < 6.0.3

Upgrade to VMware Workstation version 6.0.3

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.1.144. VMware Player: DHCP denial of service vulnerability (VMSA-2008-0005) (CVE-2008-1364) (vmsa-2008-0005-cve-2008-1364-player)

Description:

Unspecified vulnerability in the DHCP service in VMware Workstation 5.5.x before 5.5.6, VMware Player 1.0.x before 1.0.6, VMware ACE 1.0.x before 1.0.5, VMware Server 1.0.x before 1.0.5, and VMware Fusion 1.1.x before 1.1.1 allows attackers to cause a denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	28276
BID	28289
CVE	CVE-2008-1364
URL	http://www.vmware.com/security/advisories/VMSA-2008-0005.html
XF	41254

Vulnerability Solution:

VMware Player >= 1.0 and < 1.0.6

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.145. VMware Workstation: DHCP denial of service vulnerability (VMSA-2008-0005) (CVE-2008-1364) (vmsa-2008-0005-cve-2008-1364-workstation)

Description:

Unspecified vulnerability in the DHCP service in VMware Workstation 5.5.x before 5.5.6, VMware Player 1.0.x before 1.0.6, VMware ACE 1.0.x before 1.0.5, VMware Server 1.0.x before 1.0.5, and VMware Fusion 1.1.x before 1.1.1 allows attackers to cause a denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	28276
BID	28289
CVE	CVE-2008-1364
URL	http://www.vmware.com/security/advisories/VMSA-2008-0005.html
XF	41254

Vulnerability Solution:

VMware Workstation >= 5.5 and < 5.5.6
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

3.1.146. VMware Player: Update to Freetype (VMSA-2008-0014) (CVE-2008-1806) (vmsa-2008-0014-cve-2008-1806-player)

Description:

Integer overflow in FreeType2 before 2.3.6 allows context-dependent attackers to execute arbitrary code via a crafted set of 16-bit length values within the Private dictionary table in a Printer Font Binary (PFB) file, which triggers a heap-based buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Player

References:

Source	Reference
APPLE	APPLE-SA-2008-09-09
APPLE	APPLE-SA-2008-09-12
APPLE	APPLE-SA-2009-02-12
BID	29640
CVE	CVE-2008-1806
OVAL	9321
REDHAT	RHSA-2008:0556
REDHAT	RHSA-2008:0558
URL	http://www.vmware.com/security/advisories/VMSA-2008-0014.html

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.8

Upgrade to VMware Player version 1.0.8

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.0 and < 2.0.5

Upgrade to VMware Player version 2.0.5

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.147. VMware Workstation: Update to Freetype (VMSA-2008-0014) (CVE-2008-1806) (vmsa-2008-0014-cve-2008-1806-workstation)

Description:

Integer overflow in FreeType2 before 2.3.6 allows context-dependent attackers to execute arbitrary code via a crafted set of 16-bit length values within the Private dictionary table in a Printer Font Binary (PFB) file, which triggers a heap-based buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Workstation

References:

Source	Reference
APPLE	APPLE-SA-2008-09-09
APPLE	APPLE-SA-2008-09-12

Source	Reference
APPLE	APPLE-SA-2009-02-12
BID	29640
CVE	CVE-2008-1806
OVAL	9321
REDHAT	RHSA-2008:0556
REDHAT	RHSA-2008:0558
URL	http://www.vmware.com/security/advisories/VMSA-2008-0014.html

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.8

Upgrade to VMware Workstation version 5.5.8

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6 and < 6.0.5

Upgrade to VMware Workstation version 6.0.5

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.1.148. VMware Player: Update to Freetype (VMSA-2008-0014) (CVE-2008-1807) (vmsa-2008-0014-cve-2008-1807-player)

Description:

FreeType2 before 2.3.6 allow context-dependent attackers to execute arbitrary code via an invalid "number of axes" field in a Printer Font Binary (PFB) file, which triggers a free of arbitrary memory locations, leading to memory corruption.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Player

References:

Source	Reference
APPLE	APPLE-SA-2008-09-09
APPLE	APPLE-SA-2008-09-12
APPLE	APPLE-SA-2009-02-12
BID	29641
CVE	CVE-2008-1807

Source	Reference
OVAL	9767
REDHAT	RHSA-2008:0556
REDHAT	RHSA-2008:0558
URL	http://www.vmware.com/security/advisories/VMSA-2008-0014.html

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.8

Upgrade to VMware Player version 1.0.8

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.0 and < 2.0.5

Upgrade to VMware Player version 2.0.5

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.149. VMware Workstation: Update to Freetype (VMSA-2008-0014) (CVE-2008-1807) (vmsa-2008-0014-cve-2008-1807-workstation)

Description:

FreeType2 before 2.3.6 allow context-dependent attackers to execute arbitrary code via an invalid "number of axes" field in a Printer Font Binary (PFB) file, which triggers a free of arbitrary memory locations, leading to memory corruption.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Workstation

References:

Source	Reference
APPLE	APPLE-SA-2008-09-09
APPLE	APPLE-SA-2008-09-12
APPLE	APPLE-SA-2009-02-12
BID	29641
CVE	CVE-2008-1807
OVAL	9767
REDHAT	RHSA-2008:0556
REDHAT	RHSA-2008:0558

Source	Reference
URL	http://www.vmware.com/security/advisories/VMSA-2008-0014.html

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.8

Upgrade to VMware Workstation version 5.5.8

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6 and < 6.0.5

Upgrade to VMware Workstation version 6.0.5

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.1.150. VMware Player: Update to Freetype (VMSA-2008-0014) (CVE-2008-1808) (vmsa-2008-0014-cve-2008-1808-player)

Description:

Multiple off-by-one errors in FreeType2 before 2.3.6 allow context-dependent attackers to execute arbitrary code via (1) a crafted table in a Printer Font Binary (PFB) file or (2) a crafted SHC instruction in a TrueType Font (TTF) file, which triggers a heap-based buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Player

References:

Source	Reference
APPLE	APPLE-SA-2008-09-09
APPLE	APPLE-SA-2008-09-12
APPLE	APPLE-SA-2009-02-12
BID	29637
BID	29639
CVE	CVE-2008-1808
OVAL	11188
REDHAT	RHSA-2008:0556
REDHAT	RHSA-2008:0558
REDHAT	RHSA-2009:0329
URL	http://www.vmware.com/security/advisories/VMSA-2008-0014.html

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.8

Upgrade to VMware Player version 1.0.8

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.0 and < 2.0.5

Upgrade to VMware Player version 2.0.5

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.151. VMware Workstation: Update to Freetype (VMSA-2008-0014) (CVE-2008-1808) (vmsa-2008-0014-cve-2008-1808-workstation)

Description:

Multiple off-by-one errors in FreeType2 before 2.3.6 allow context-dependent attackers to execute arbitrary code via (1) a crafted table in a Printer Font Binary (PFB) file or (2) a crafted SHC instruction in a TrueType Font (TTF) file, which triggers a heap-based buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Workstation

References:

Source	Reference
APPLE	APPLE-SA-2008-09-09
APPLE	APPLE-SA-2008-09-12
APPLE	APPLE-SA-2009-02-12
BID	29637
BID	29639
CVE	CVE-2008-1808
OVAL	11188
REDHAT	RHSA-2008:0556
REDHAT	RHSA-2008:0558
REDHAT	RHSA-2009:0329
URL	http://www.vmware.com/security/advisories/VMSA-2008-0014.html

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.8

Upgrade to VMware Workstation version 5.5.8

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6 and < 6.0.5

Upgrade to VMware Workstation version 6.0.5

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.1.152. VMware Player: Third party libpng updated to version 1.2.44 (VMSA-2010-0014) (CVE-2010-0205) (vmsa-2010-0014-cve-2010-0205-player)

Description:

The png_decompress_chunk function in pngrutil.c in libpng 1.0.x before 1.0.53, 1.2.x before 1.2.43, and 1.4.x before 1.4.1 does not properly handle compressed ancillary-chunk data that has a disproportionately large uncompressed representation, which allows remote attackers to cause a denial of service (memory and CPU consumption, and application hang) via a crafted PNG file, as demonstrated by use of the deflate compression method on data composed of many occurrences of the same character, related to a "decompression bomb" attack.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
APPLE	APPLE-SA-2010-11-10-1
BID	38478
CERT-VN	576029
CVE	CVE-2010-0205
DEBIAN	DSA-2032
URL	http://www.vmware.com/security/advisories/VMSA-2010-0014.html
XF	56661

Vulnerability Solution:

•VMware Player >= 2.5 and < 2.5.5

Upgrade to VMware Player version 2.5.5

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 3.1 and < 3.1.2

Upgrade to VMware Player version 3.1.2

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.153. VMware Workstation: Third party libpng updated to version 1.2.44 (VMSA-2010-0014) (CVE-2010-0205) (vmsa-2010-0014-cve-2010-0205-workstation)

Description:

The png_decompress_chunk function in pngrutil.c in libpng 1.0.x before 1.0.53, 1.2.x before 1.2.43, and 1.4.x before 1.4.1 does not properly handle compressed ancillary-chunk data that has a disproportionately large uncompressed representation, which allows remote attackers to cause a denial of service (memory and CPU consumption, and application hang) via a crafted PNG file, as demonstrated by use of the deflate compression method on data composed of many occurrences of the same character, related to a "decompression bomb" attack.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
APPLE	APPLE-SA-2010-11-10-1
BID	38478
CERT-VN	576029
CVE	CVE-2010-0205
DEBIAN	DSA-2032
URL	http://www.vmware.com/security/advisories/VMSA-2010-0014.html
XF	56661

Vulnerability Solution:

•VMware Workstation >= 6.5 and < 6.5.5

Upgrade to VMware Workstation version 6.5.5

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

•VMware Workstation >= 7 and < 7.1.2

Upgrade to VMware Workstation version 7.1.2

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.1.154. VMware Player: Third party libpng updated to version 1.2.44 (VMSA-2010-0014) (CVE-2010-1205) (vmsa-2010-0014-cve-2010-1205-player)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

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
DEBIAN	DSA-2072
OVAL	11851
URL	http://www.vmware.com/security/advisories/VMSA-2010-0014.html
XF	59815

Vulnerability Solution:

•VMware Player >= 2.5 and < 2.5.5

Upgrade to VMware Player version 2.5.5

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 3.1 and < 3.1.2

Upgrade to VMware Player version 3.1.2

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.155. VMware Workstation: Third party libpng updated to version 1.2.44 (VMSA-2010-0014) (CVE-2010-1205) (vmsa-2010-0014-cve-2010-1205-workstation)

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:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

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
DEBIAN	DSA-2072
OVAL	11851
URL	http://www.vmware.com/security/advisories/VMSA-2010-0014.html
XF	59815

Vulnerability Solution:

•VMware Workstation >= 6.5 and < 6.5.5

Upgrade to VMware Workstation version 6.5.5

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

•VMware Workstation >= 7 and < 7.1.2

Upgrade to VMware Workstation version 7.1.2

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.1.156. VMware Player: VMware ROM Overwrite Privilege Escalation (VMSA-2012-0006) (CVE-2012-1515) (vmsa-2012-0006-cve-2012-1515-player)

Description:

VMware ESXi 3.5, 4.0, and 4.1 and ESX 3.5, 4.0, and 4.1 do not properly implement port-based I/O operations, which allows guest OS users to gain guest OS privileges by overwriting memory locations in a read-only memory block associated with the Virtual DOS Machine.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	52820
CERT	TA12-164A
CVE	CVE-2012-1515
DISA_SEVERITY	Category I
DISA_VMSKEY	V0031979
IAVM	2012-A-0056
MS	MS12-042
OVAL	15209
OVAL	17110
URL	http://www.vmware.com/security/advisories/VMSA-2012-0006.html
XF	74480

Vulnerability Solution:

VMware Player >= 3.1 and < 3.1.2
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.157. VMware Workstation: VMware ROM Overwrite Privilege Escalation (VMSA-2012-0006) (CVE-2012-1515) (vmsa-2012-0006-cve-2012-1515-workstation)

Description:

VMware ESXi 3.5, 4.0, and 4.1 and ESX 3.5, 4.0, and 4.1 do not properly implement port-based I/O operations, which allows guest OS users to gain guest OS privileges by overwriting memory locations in a read-only memory block associated with the Virtual DOS Machine.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	52820
CERT	TA12-164A
CVE	CVE-2012-1515
DISA_SEVERITY	Category I

Source	Reference
DISA_VMSKEY	V0031979
IAVM	2012-A-0056
MS	MS12-042
OVAL	15209
OVAL	17110
URL	http://www.vmware.com/security/advisories/VMSA-2012-0006.html
XF	74480

Vulnerability Solution:

VMware Workstation >= 7 and < 7.1.2
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.1.158. VMware Player: VMware Tools Incorrect Folder Permissions Privilege Escalation (VMSA-2012-0007) (CVE-2012-1518) (vmsa-2012-0007-cve-2012-1518-player)

Description:

VMware Workstation 8.x before 8.0.2, VMware Player 4.x before 4.0.2, VMware Fusion 4.x before 4.1.2, VMware ESXi 3.5 through 5.0, and VMware ESX 3.5 through 4.1 use an incorrect ACL for the VMware Tools folder, which allows guest OS users to gain guest OS privileges via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	53006
CVE	CVE-2012-1518
DISA_SEVERITY	Category I
DISA_VMSKEY	V0032167
DISA_VMSKEY	V0032171
IAVM	2012-A-0072
IAVM	2012-A-0073
OSVDB	81163
OVAL	16745
URL	http://www.vmware.com/security/advisories/VMSA-2012-0007.html

Vulnerability Solution:

•VMware Player >= 3.1 and < 3.1.6

Upgrade to VMware Player version 3.1.6

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 4.0 and < 4.0.2

Upgrade to VMware Player version 4.0.2

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.159. VMware Workstation: VMware Tools Incorrect Folder Permissions Privilege Escalation (VMSA-2012-0007) (CVE-2012-1518) (vmsa-2012-0007-cve-2012-1518-workstation)

Description:

VMware Workstation 8.x before 8.0.2, VMware Player 4.x before 4.0.2, VMware Fusion 4.x before 4.1.2, VMware ESXi 3.5 through 5.0, and VMware ESX 3.5 through 4.1 use an incorrect ACL for the VMware Tools folder, which allows guest OS users to gain guest OS privileges via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	53006
CVE	CVE-2012-1518
DISA_SEVERITY	Category I
DISA_VMSKEY	V0032167
DISA_VMSKEY	V0032171
IAVM	2012-A-0072
IAVM	2012-A-0073
OSVDB	81163
OVAL	16745
URL	http://www.vmware.com/security/advisories/VMSA-2012-0007.html

Vulnerability Solution:

•VMware Workstation >= 7 and < 7.1.6

Upgrade to VMware Workstation version 7.1.6

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

•VMware Workstation >= 8 and < 8.0.2

Upgrade to VMware Workstation version 8.0.2

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/8_0

3.1.160. VMware Player: VMware Virtual Machine Remote Device Denial of Service (VMSA-2012-0011) (CVE-2012-3289) (vmsa-2012-0011-cve-2012-3289-player)

Description:

VMware Workstation 8.x before 8.0.4, VMware Player 4.x before 4.0.4, VMware ESXi 3.5 through 5.0, and VMware ESX 3.5 through 4.1 allow remote attackers to cause a denial of service (guest OS crash) via crafted traffic from a remote virtual device.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
CVE	CVE-2012-3289
DISA_SEVERITY	Category I
DISA_VMSKEY	V0032846
DISA_VMSKEY	V0032847
IAVM	2012-A-0099
IAVM	2012-A-0100
URL	http://www.vmware.com/security/advisories/VMSA-2012-0011.html

Vulnerability Solution:

VMware Player >= 4.0 and < 4.0.4
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.161. VMware Workstation: VMware Virtual Machine Remote Device Denial of Service (VMSA-2012-0011) (CVE-2012-3289) (vmsa-2012-0011-cve-2012-3289-workstation)

Description:

VMware Workstation 8.x before 8.0.4, VMware Player 4.x before 4.0.4, VMware ESXi 3.5 through 5.0, and VMware ESX 3.5 through 4.1 allow remote attackers to cause a denial of service (guest OS crash) via crafted traffic from a remote virtual device.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
CVE	CVE-2012-3289
DISA_SEVERITY	Category I
DISA_VMSKEY	V0032846
DISA_VMSKEY	V0032847
IAVM	2012-A-0099
IAVM	2012-A-0100
URL	http://www.vmware.com/security/advisories/VMSA-2012-0011.html

Vulnerability Solution:

VMware Workstation >= 8 and < 8.0.4
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/8_0

3.1.162. VMware Workstation: VMware LGTOSYNC privilege escalation (VMSA-2013-0014) (CVE-2013-3519) (vmsa-2013-0014-cve-2013-3519-workstation)

Description:

lgtosync.sys in VMware Workstation 9.x before 9.0.3, VMware Player 5.x before 5.0.3, VMware Fusion 5.x before 5.0.4, VMware ESXi 4.0 through 5.1, and VMware ESX 4.0 and 4.1, when a 32-bit Windows guest OS is used, allows guest OS users to gain guest OS privileges via an application that performs a crafted memory allocation.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
CVE	CVE-2013-3519
URL	http://www.vmware.com/security/advisories/VMSA-2013-0014.html

Vulnerability Solution:

VMware Workstation >= 9 and < 9.0.3
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/9_0

3.1.163. VMware Player: Vulnerability (VMSA-2015-0004) (CVE-2015-2341) (vmsa-2015-0004-cve-2015-2341-player)

Description:

VMware Workstation 10.x before 10.0.5, VMware Player 6.x before 6.0.6, and VMware Fusion 6.x before 6.0.6 and 7.x before 7.0.1 allow attackers to cause a denial of service against a 32-bit guest OS or 64-bit host OS via a crafted RPC command.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	75094
CVE	CVE-2015-2341
DISA_SEVERITY	Category I
DISA_VMSKEY	V0060979
IAVM	2015-B-0077
URL	http://www.vmware.com/security/advisories/VMSA-2015-0004.html

Vulnerability Solution:
VMware Player >= 6.0 and < 6.0.6
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.164. VMware Workstation: Vulnerability (VMSA-2015-0004) (CVE-2015-2341) (vmsa-2015-0004-cve-2015-2341-workstation)

Description:

VMware Workstation 10.x before 10.0.5, VMware Player 6.x before 6.0.6, and VMware Fusion 6.x before 6.0.6 and 7.x before 7.0.1 allow attackers to cause a denial of service against a 32-bit guest OS or 64-bit host OS via a crafted RPC command.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	75094
CVE	CVE-2015-2341
DISA_SEVERITY	Category I
DISA_VMSKEY	V0060979
IAVM	2015-B-0077
URL	http://www.vmware.com/security/advisories/VMSA-2015-0004.html

Vulnerability Solution:

VMware Workstation >= 10 and < 10.0.5
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

3.1.165. VMware Player: VMware Workstation and Fusion updates address out-of-bounds memory access vulnerability (VMSA-2017-0005) (CVE-2017-4901) (vmsa-2017-0005-cve-2017-4901-player)

Description:

The drag-and-drop (DnD) function in VMware Workstation 12.x before version 12.5.4 and Fusion 8.x before version 8.5.5 has an out-of-bounds memory access vulnerability. This may allow a guest to execute code on the operating system that runs Workstation or Fusion.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	96881
CVE	CVE-2017-4901
URL	http://www.vmware.com/security/advisories/VMSA-2017-0005.html

Vulnerability Solution:

VMware Player >= 12.5 and < 12.5.4
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.1.166. VMware Workstation: VMware Workstation and Fusion updates address out-of-bounds memory access vulnerability (VMSA-2017-0005) (CVE-2017-4901) (vmsa-2017-0005-cve-2017-4901-workstation)

Description:

The drag-and-drop (DnD) function in VMware Workstation 12.x before version 12.5.4 and Fusion 8.x before version 8.5.5 has an out-of-bounds memory access vulnerability. This may allow a guest to execute code on the operating system that runs Workstation or Fusion.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	96881
CVE	CVE-2017-4901
URL	http://www.vmware.com/security/advisories/VMSA-2017-0005.html

Vulnerability Solution:
VMware Workstation >= 12.5 and < 12.5.4
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

3.2. Severe Vulnerabilities

3.2.1. Apache HTTPD: mod_proxy reverse proxy DoS (CVE-2009-1890) (apache-httpd-cve-2009-1890)

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. A denial of service flaw was found in the mod_proxy module when it was used as a reverse proxy. A remote attacker could use this flaw to force a proxy process to consume large amounts of CPU time.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2009-11-09-1
BID	35565

Source	Reference
CVE	CVE-2009-1890
DEBIAN	DSA-1834
OVAL	12330
OVAL	8616
OVAL	9403
REDHAT	RHSA-2009:1148
REDHAT	RHSA-2009:1156
SUSE	SUSE-SA:2009:050
URL	http://httpd.apache.org/security/vulnerabilities_22.html

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.

3.2.2. Apache HTTPD: mod_deflate DoS (CVE-2009-1891) (apache-httpd-cve-2009-1891)

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 denial of service flaw was found in the mod_deflate module. This module continued to compress large files until compression was complete, even if the network connection that requested the content was closed before compression completed. This would cause mod_deflate to consume large amounts of CPU if mod_deflate was enabled for a large file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2009-11-09-1
CVE	CVE-2009-1891
DEBIAN	DSA-1834
OVAL	12361
OVAL	8632

Source	Reference
OVAL	9248
REDHAT	RHSA-2009:1148
REDHAT	RHSA-2009:1156
SUSE	SUSE-SA:2009:050
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.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 < 2.2.12

Upgrade to Apache HTTPD version 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.

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

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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

Source	Reference
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
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.

3.2.4. 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.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:443	The subject common name found in the X.509 certificate does not seem to match the scan target:Subject CN localhost does not match target name specified in the site.Subject CN resolved IP address differs from node IP address specified in the site.Subject CN resolved IP address differs from node IP address specified in the site.
192.168.234.131:5432	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.

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

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:139	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian
192.168.234.131:445	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
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.

3.2.6. SMB signing disabled (cifs-smb-signing-disabled)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:139	SMB signing is disabled
192.168.234.130:445	SMB signing is disabled
192.168.234.131:139	SMB signing is disabled
192.168.234.131:445	SMB signing is disabled

References:

Source	Reference

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

3.2.7. ISC BIND: Specific APL data could trigger an INSIST in apl_42.c (CVE-2015-8704) (dns-bind-cve-2015-8704)

Description:

apl_42.c in ISC BIND 9.x before 9.9.8-P3, 9.9.x, and 9.10.x before 9.10.3-P3 allows remote authenticated users to cause a denial of service (INSIST assertion failure and daemon exit) via a malformed Address Prefix List (APL) record.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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	81329

Source	Reference
CVE	CVE-2015-8704
DEBIAN	DSA-3449
REDHAT	RHSA-2016:0073
REDHAT	RHSA-2016:0074
URL	https://kb.isc.org/article/AA-01335/0

Vulnerability Solution:

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

3.2.8. CVE-2009-0025: EVP_VerifyFinal() and DSA_do_verify() return checks (dns-bind-ssl-signature-spoofing)

Description:

BIND 9.6.0, 9.5.1, 9.5.0, 9.4.3, and earlier does not properly check the return value from the OpenSSL DSA_verify function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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-2009-05-12
BID	33151
CERT	TA09-133A
CVE	CVE-2009-0025
OVAL	10879
OVAL	5569
URL	https://kb.isc.org/article/AA-00925/187/CVE-2009-0025%3A-EVP_VerifyFinal-and-DSA_do_verify-return-checks.html

Vulnerability Solution:

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

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

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:21	Running FTP serviceConfiguration item ftp.plaintext.authentication set to 'true' matched
192.168.234.131:21	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.

3.2.10. MySQL Directory Traversal and Arbitrary Table Access Vulnerability (mysql-directory-traversal-and-arbitrary-table-access)

Description:

Directory traversal vulnerability in MySQL 5.0 through 5.0.91 and 5.1 before 5.1.47 allows remote authenticated users to bypass intended table grants to read field definitions of arbitrary tables, and on 5.1 to read or delete content of arbitrary tables, via a .. (dot dot) in a table name.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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-2010-11-10-1
CVE	CVE-2010-1848

Source	Reference
OVAL	10258
OVAL	7210
REDHAT	RHSA-2010:0442
REDHAT	RHSA-2010:0824
URL	http://bugs.mysql.com/bug.php?id=53371
URL	http://dev.mysql.com/doc/refman/5.0/en/news-5-0-91.html
URL	http://dev.mysql.com/doc/refman/5.1/en/news-5-1-47.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.91

Upgrade to Oracle MySQL version 5.0.91

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 < 5.1.47

Upgrade to Oracle MySQL version 5.1.47

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

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

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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

Source	Reference
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.

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

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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.

3.2.13. PHP Vulnerability: CVE-2009-3558 (php-cve-2009-3558)

Description:

The posix_mkfifo function in ext/posix/posix.c in PHP before 5.2.12 and 5.3.x before 5.3.1 allows context-dependent attackers to bypass open_basedir restrictions, and create FIFO files, via the pathname and mode arguments, as demonstrated by creating a .htaccess file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
CVE	CVE-2009-3558

Vulnerability Solution:

•Upgrade to PHP version 5.2.12

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

•Upgrade to PHP version 5.3.1

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

3.2.14. PHP Vulnerability: CVE-2009-5016 (php-cve-2009-5016)

Description:

Integer overflow in the xml_utf8_decode function in ext/xml/xml.c in PHP before 5.2.11 makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string that uses overlong UTF-8 encoding, a different vulnerability than CVE-2010-3870.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	44889
CVE	CVE-2009-5016
REDHAT	RHSA-2010:0919
REDHAT	RHSA-2011:0195

Vulnerability Solution:

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

3.2.15. PHP Vulnerability: CVE-2010-3870 (php-cve-2010-3870)

Description:

The utf8_decode function in PHP before 5.3.4 does not properly handle non-shortest form UTF-8 encoding and ill-formed subsequences in UTF-8 data, which makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
BID	44605
CVE	CVE-2010-3870
REDHAT	RHSA-2010:0919
REDHAT	RHSA-2011:0195

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.16. PHP Vulnerability: CVE-2014-3670 (php-cve-2014-3670)

Description:

The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
BID	70665
CVE	CVE-2014-3670
DEBIAN	DSA-3064
REDHAT	RHSA-2014:1765
REDHAT	RHSA-2014:1766
REDHAT	RHSA-2014:1767
REDHAT	RHSA-2014:1768
REDHAT	RHSA-2014:1824
URL	https://bugs.php.net/bug.php?id=68113

Vulnerability Solution:

•Upgrade to PHP version 5.4.34

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

•Upgrade to PHP version 5.5.18

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

•Upgrade to PHP version 5.6.2

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

3.2.17. PHP Vulnerability: CVE-2015-7803 (php-cve-2015-7803)

Description:

The phar_get_entry_data function in ext/phar/util.c in PHP before 5.5.30 and 5.6.x before 5.6.14 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a .phar file with a crafted TAR archive entry in which the Link indicator references a file that does not exist.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2015-12-08-3
BID	76959
CVE	CVE-2015-7803
DEBIAN	DSA-3380
URL	https://bugs.php.net/bug.php?id=69720

Vulnerability Solution:

•Upgrade to PHP version 5.5.30

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

•Upgrade to PHP version 5.6.14

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

3.2.18. PHP Vulnerability: CVE-2015-7804 (php-cve-2015-7804)

Description:

Off-by-one error in the phar_parse_zipfile function in ext/phar/zip.c in PHP before 5.5.30 and 5.6.x before 5.6.14 allows remote attackers to cause a denial of service (uninitialized pointer dereference and application crash) by including the / filename in a .zip PHAR archive.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2015-12-08-3
BID	76959
CVE	CVE-2015-7804
DEBIAN	DSA-3380
URL	https://bugs.php.net/bug.php?id=70433

Vulnerability Solution:

•Upgrade to PHP version 5.5.30

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

•Upgrade to PHP version 5.6.14

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

3.2.19. 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:
192.168.234.131:80	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	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/

3.2.20. PHP Vulnerability: CVE-2016-5399 (php-cve-2016-5399)

Description:

The bzread function in ext/bz2/bz2.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted bz2 archive.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	92051
CVE	CVE-2016-5399
DEBIAN	DSA-3631
REDHAT	RHSA-2016:2598
REDHAT	RHSA-2016:2750
URL	https://bugs.php.net/bug.php?id=72613

Vulnerability Solution:

•Upgrade to PHP version 5.5.38

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

•Upgrade to PHP version 5.6.24

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

•Upgrade to PHP version 7.0.9

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

3.2.21. PHP Vulnerability: CVE-2016-6174 (php-cve-2016-6174)

Description:

applications/core/modules/front/system/content.php in Invision Power Services IPS Community Suite (aka Invision Power Board, IPB, or Power Board) before 4.1.13, when used with PHP before 5.4.24 or 5.5.x before 5.5.8, allows remote attackers to execute arbitrary code via the content_class parameter.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2016-09-20
BID	91732
CVE	CVE-2016-6174

Vulnerability Solution:

•Upgrade to PHP version 5.4.24

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

•Upgrade to PHP version 5.5.8

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

3.2.22. PHP Vulnerability: CVE-2016-6289 (php-cve-2016-6289)

Description:

Integer overflow in the virtual_file_ex function in TSRM/tsrm_virtual_cwd.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted extract operation on a ZIP archive.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2016-09-20
BID	92074
CVE	CVE-2016-6289
DEBIAN	DSA-3631
REDHAT	RHSA-2016:2750
URL	https://bugs.php.net/72513

Vulnerability Solution:

•Upgrade to PHP version 5.5.38
Download and apply the upgrade from: http://www.php.net/releases/
•Upgrade to PHP version 5.6.24
Download and apply the upgrade from: http://www.php.net/releases/
•Upgrade to PHP version 7.0.9
Download and apply the upgrade from: http://www.php.net/releases/

3.2.23. PHP Vulnerability: CVE-2017-11628 (php-cve-2017-11628)

Description:

In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, a stack-based buffer overflow in the zend_ini_do_op() function in Zend/zend_ini_parser.c could cause a denial of service or potentially allow executing code. NOTE: this is only relevant for PHP applications that accept untrusted input (instead of the system's php.ini file) for the parse_ini_string or parse_ini_file function, e.g., a web application for syntax validation of php.ini directives.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	99489
CVE	CVE-2017-11628
DEBIAN	DSA-4080
DEBIAN	DSA-4081
URL	https://bugs.php.net/bug.php?id=74603

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/

3.2.24. 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:
192.168.234.131:5432	The certificate is not valid after Fri, 16 Apr 2010 17:07:45 EEST

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.

3.2.25. Anonymous root login is allowed (unix-anonymous-root-logins)

Description:

Anonymous root logins should only be allowed from system console. /etc/securetty allows you to specify on which tty's and virtual consoles root is allowed to login. The tty and vc's listed in this file will allow root to login on certain tty's and VC's. On other tty or vc's root user will not be allowed and user has to "su" to become root.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Following entries in /etc/securetty may allow anonymous root logins: -rw-r--r-- 1 root root 886 Apr 16 2010 /etc/group

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.

3.2.26. VMware Player: Arbitrary code execution and denial of service vulnerabilities (VMSA-2007-0006) (CVE-2007-4496) (vmsa-2007-0006-cve-2007-4496-player)

Description:

Unspecified vulnerability in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 55017, Player before 1.0.5 Build 56455 and Player 2 before 2.0.1 Build 55017, ACE before 1.0.3 Build 54075 and ACE 2 before 2.0.1 Build 55017, and Server before 1.0.4 Build 56528 allows authenticated users with administrative privileges on a guest operating system to corrupt memory and possibly execute arbitrary code on the host operating system via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	25728
CVE	CVE-2007-4496
URL	http://www.vmware.com/security/advisories/VMSA-2007-0006.html

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.5

Upgrade to VMware Player version 1.0.5

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.0 and < 2.0.1

Upgrade to VMware Player version 2.0.1

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.27. VMware Workstation: Arbitrary code execution and denial of service vulnerabilities (VMSA-2007-0006) (CVE-2007-4496) (vmsa-2007-0006-cve-2007-4496-workstation)

Description:

Unspecified vulnerability in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 55017, Player before 1.0.5 Build 56455 and Player 2 before 2.0.1 Build 55017, ACE before 1.0.3 Build 54075 and ACE 2 before 2.0.1 Build 55017, and Server before 1.0.4 Build 56528 allows authenticated users with administrative privileges on a guest operating system to corrupt memory and possibly execute arbitrary code on the host operating system via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	25728
CVE	CVE-2007-4496
URL	http://www.vmware.com/security/advisories/VMSA-2007-0006.html

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.5

Upgrade to VMware Workstation version 5.5.5

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6 and < 6.0.1

Upgrade to VMware Workstation version 6.0.1

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.2.28. VMware Player: Virtual Machine Communication Interface (VMCI) memory corruption resulting in denial of service (VMSA-2008-0005) (CVE-2008-1340) (vmsa-2008-0005-cve-2008-1340-player)

Description:

Virtual Machine Communication Interface (VMCI) in VMware Workstation 6.0.x before 6.0.3, VMware Player 2.0.x before 2.0.3, and VMware ACE 2.0.x before 2.0.1 allows attackers to cause a denial of service (host OS crash) via crafted VMCI calls that trigger "memory exhaustion and memory corruption."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	28276
BID	28289
CVE	CVE-2008-1340
URL	http://www.vmware.com/security/advisories/VMSA-2008-0005.html
XF	41250

Vulnerability Solution:

VMware Player >= 2.0 and < 2.0.3

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.29. VMware Workstation: Virtual Machine Communication Interface (VMCI) memory corruption resulting in denial of service (VMSA-2008-0005) (CVE-2008-1340) (vmsa-2008-0005-cve-2008-1340-workstation)

Description:

Virtual Machine Communication Interface (VMCI) in VMware Workstation 6.0.x before 6.0.3, VMware Player 2.0.x before 2.0.3, and VMware ACE 2.0.x before 2.0.1 allows attackers to cause a denial of service (host OS crash) via crafted VMCI calls that trigger "memory exhaustion and memory corruption."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	28276
BID	28289
CVE	CVE-2008-1340
URL	http://www.vmware.com/security/advisories/VMSA-2008-0005.html
XF	41250

Vulnerability Solution:

VMware Workstation >= 6 and < 6.0.3
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.2.30. VMware Player: VMware HGFS File System Heap Overflow (VMSA-2008-0008) (CVE-2008-2098) (vmsa-2008-0008-cve-2008-2098-player)

Description:

Heap-based buffer overflow in the VMware Host Guest File System (HGFS) in VMware Workstation 6 before 6.0.4 build 93057, VMware Player 2 before 2.0.4 build 93057, VMware ACE 2 before 2.0.2 build 93057, and VMware Fusion before 1.1.2 build 87978, when folder sharing is used, allows guest OS users to execute arbitrary code on the host OS via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
CVE	CVE-2008-2098
URL	http://www.vmware.com/security/advisories/VMSA-2008-0008.html

Source	Reference
XF	42753

Vulnerability Solution:

VMware Player >= 2.0 and < 2.0.4
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.31. VMware Workstation: VMware HGFS File System Heap Overflow (VMSA-2008-0008) (CVE-2008-2098) (vmsa-2008-0008-cve-2008-2098-workstation)

Description:

Heap-based buffer overflow in the VMware Host Guest File System (HGFS) in VMware Workstation 6 before 6.0.4 build 93057, VMware Player 2 before 2.0.4 build 93057, VMware ACE 2 before 2.0.2 build 93057, and VMware Fusion before 1.1.2 build 87978, when folder sharing is used, allows guest OS users to execute arbitrary code on the host OS via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
CVE	CVE-2008-2098
URL	http://www.vmware.com/security/advisories/VMSA-2008-0008.html
XF	42753

Vulnerability Solution:

VMware Workstation >= 6 and < 6.0.4
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.2.32. VMware Player: Privilege escalation on ESX or Linux based hosted operating systems (VMSA-2008-0009) (CVE-2008-0967) (vmsa-2008-0009-cve-2008-0967-player)

Description:

Untrusted search path vulnerability in vmware-authd in VMware Workstation 5.x before 5.5.7 build 91707 and 6.x before 6.0.4 build 93057, VMware Player 1.x before 1.0.7 build 91707 and 2.x before 2.0.4 build 93057, and VMware Server before 1.0.6 build 91891 on Linux, and VMware ESXi 3.5 and VMware ESX 2.5.4 through 3.5, allows local users to gain privileges via a library path option in a configuration file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Player

References:

Source	Reference
BID	29557
CVE	CVE-2008-0967
OVAL	4768
OVAL	5583
URL	http://www.vmware.com/security/advisories/VMSA-2008-0009.html
XF	42878

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.7

Upgrade to VMware Player version 1.0.7

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.0 and < 2.0.4

Upgrade to VMware Player version 2.0.4

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.33. VMware Workstation: Privilege escalation on ESX or Linux based hosted operating systems (VMSA-2008-0009) (CVE-2008-0967) (vmsa-2008-0009-cve-2008-0967-workstation)

Description:

Untrusted search path vulnerability in vmware-authd in VMware Workstation 5.x before 5.5.7 build 91707 and 6.x before 6.0.4 build 93057, VMware Player 1.x before 1.0.7 build 91707 and 2.x before 2.0.4 build 93057, and VMware Server before 1.0.6 build 91891 on Linux, and VMware ESXi 3.5 and VMware ESX 2.5.4 through 3.5, allows local users to gain privileges via a library path option in a configuration file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	29557
CVE	CVE-2008-0967
OVAL	4768
OVAL	5583
URL	http://www.vmware.com/security/advisories/VMSA-2008-0009.html
XF	42878

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.7

Upgrade to VMware Workstation version 5.5.7

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6 and < 6.0.4

Upgrade to VMware Workstation version 6.0.4

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.2.34. VMware Player: VMware VIX Application Programming Interface (API) Memory Overflow Vulnerabilities (VMSA-2008-0009) (CVE-2008-2100) (vmsa-2008-0009-cve-2008-2100-player)

Description:

Multiple buffer overflows in VIX API 1.1.x before 1.1.4 build 93057 on VMware Workstation 5.x and 6.x, VMware Player 1.x and 2.x, VMware ACE 2.x, VMware Server 1.x, VMware Fusion 1.x, VMware ESXi 3.5, and VMware ESX 3.0.1 through 3.5 allow guest OS users to execute arbitrary code on the host OS via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	29552
CVE	CVE-2008-2100
OVAL	5081
OVAL	5647
URL	http://www.vmware.com/security/advisories/VMSA-2008-0009.html
XF	42872

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.6

Upgrade to VMware Player version 1.0.6

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.0 and < 2.0.4

Upgrade to VMware Player version 2.0.4

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.35. VMware Workstation: VMware VIX Application Programming Interface (API) Memory Overflow Vulnerabilities (VMSA-2008-0009) (CVE-2008-2100) (vmsa-2008-0009-cve-2008-2100-workstation)

Description:

Multiple buffer overflows in VIX API 1.1.x before 1.1.4 build 93057 on VMware Workstation 5.x and 6.x, VMware Player 1.x and 2.x, VMware ACE 2.x, VMware Server 1.x, VMware Fusion 1.x, VMware ESXi 3.5, and VMware ESX 3.0.1 through 3.5 allow guest OS users to execute arbitrary code on the host OS via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	29552
CVE	CVE-2008-2100
OVAL	5081
OVAL	5647
URL	http://www.vmware.com/security/advisories/VMSA-2008-0009.html
XF	42872

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.7

Upgrade to VMware Workstation version 5.5.7

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6 and < 6.0.4

Upgrade to VMware Workstation version 6.0.4

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.2.36. VMware Player: Update to Cairo (VMSA-2008-0014) (CVE-2007-5503) (vmsa-2008-0014-cve-2007-5503-player)

Description:

Multiple integer overflows in Cairo before 1.4.12 might allow remote attackers to execute arbitrary code, as demonstrated using a crafted PNG image with large width and height values, which is not properly handled by the read_png function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Player

References:

Source	Reference
BID	26650
CVE	CVE-2007-5503
DEBIAN	DSA-1542
OVAL	11251
REDHAT	RHSA-2007:1078
URL	http://www.vmware.com/security/advisories/VMSA-2008-0014.html
XF	38771

Vulnerability Solution:

VMware Player >= 2.0 and < 2.0.5
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.37. VMware Workstation: Update to Cairo (VMSA-2008-0014) (CVE-2007-5503) (vmsa-2008-0014-cve-2007-5503-workstation)

Description:

Multiple integer overflows in Cairo before 1.4.12 might allow remote attackers to execute arbitrary code, as demonstrated using a crafted PNG image with large width and height values, which is not properly handled by the read_png function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	26650
CVE	CVE-2007-5503
DEBIAN	DSA-1542
OVAL	11251
REDHAT	RHSA-2007:1078
URL	http://www.vmware.com/security/advisories/VMSA-2008-0014.html
XF	38771

Vulnerability Solution:

VMware Workstation >= 6 and < 6.0.5

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.2.38. VMware Player: Privilege escalation on 64-bit guest operating systems (VMSA-2008-0016) (CVE-2008-4279) (vmsa-2008-0016-cve-2008-4279-player)

Description:

The CPU hardware emulation for 64-bit guest operating systems in VMware Workstation 6.0.x before 6.0.5 build 109488 and 5.x before 5.5.8 build 108000; Player 2.0.x before 2.0.5 build 109488 and 1.x before 1.0.8; Server 1.x before 1.0.7 build 108231; and ESX 2.5.4 through 3.5 allows authenticated guest OS users to gain additional guest OS privileges by triggering an exception that causes the virtual CPU to perform an indirect jump to a non-canonical address.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	31569
CVE	CVE-2008-4279
OVAL	5929
URL	http://www.vmware.com/security/advisories/VMSA-2008-0016.html
XF	45668

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.8

Upgrade to VMware Player version 1.0.8

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.0 and < 2.0.5

Upgrade to VMware Player version 2.0.5

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.39. VMware Workstation: Privilege escalation on 64-bit guest operating systems (VMSA-2008-0016) (CVE-2008-4279) (vmsa-2008-0016-cve-2008-4279-workstation)

Description:

The CPU hardware emulation for 64-bit guest operating systems in VMware Workstation 6.0.x before 6.0.5 build 109488 and 5.x before 5.5.8 build 108000; Player 2.0.x before 2.0.5 build 109488 and 1.x before 1.0.8; Server 1.x before 1.0.7 build 108231; and ESX 2.5.4 through 3.5 allows authenticated guest OS users to gain additional guest OS privileges by triggering an exception that causes the virtual CPU to perform an indirect jump to a non-canonical address.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	31569
CVE	CVE-2008-4279
OVAL	5929
URL	http://www.vmware.com/security/advisories/VMSA-2008-0016.html
XF	45668

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.8

Upgrade to VMware Workstation version 5.5.8

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6 and < 6.0.5

Upgrade to VMware Workstation version 6.0.5

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.2.40. VMware Player: A privilege escalation on 32-bit and 64-bit guest operating systems (VMSA-2008-0018) (CVE-2008-4915) (vmsa-2008-0018-cve-2008-4915-player)

Description:

The CPU hardware emulation in VMware Workstation 6.0.5 and earlier and 5.5.8 and earlier; Player 2.0.x through 2.0.5 and 1.0.x through 1.0.8; ACE 2.0.x through 2.0.5 and earlier, and 1.0.x through 1.0.7; Server 1.0.x through 1.0.7; ESX 2.5.4 through 3.5; and ESXi 3.5, when running 32-bit and 64-bit guest operating systems, does not properly handle the Trap flag, which allows authenticated guest OS users to gain privileges on the guest OS.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	32168
CVE	CVE-2008-4915
OVAL	6309
URL	http://www.vmware.com/security/advisories/VMSA-2008-0018.html
XF	46415

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.9

Upgrade to VMware Player version 1.0.9

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player < 2.5.0

Upgrade to VMware Player version 2.5.0

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.41. VMware Workstation: A privilege escalation on 32-bit and 64-bit guest operating systems (VMSA-2008-0018) (CVE-2008-4915) (vmsa-2008-0018-cve-2008-4915-workstation)

Description:

The CPU hardware emulation in VMware Workstation 6.0.5 and earlier and 5.5.8 and earlier; Player 2.0.x through 2.0.5 and 1.0.x through 1.0.8; ACE 2.0.x through 2.0.5 and earlier, and 1.0.x through 1.0.7; Server 1.0.x through 1.0.7; ESX 2.5.4 through 3.5; and ESXi 3.5, when running 32-bit and 64-bit guest operating systems, does not properly handle the Trap flag, which allows authenticated guest OS users to gain privileges on the guest OS.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	32168
CVE	CVE-2008-4915
OVAL	6309
URL	http://www.vmware.com/security/advisories/VMSA-2008-0018.html
XF	46415

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.9

Upgrade to VMware Workstation version 5.5.9

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation < 6.5.0

Upgrade to VMware Workstation version 6.5.0

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

3.2.42. VMware Player: Critical Memory corruption vulnerability (VMSA-2008-0019) (CVE-2008-4917) (vmsa-2008-0019-cve-2008-4917-player)

Description:

Unspecified vulnerability in VMware Workstation 5.5.8 and earlier, and 6.0.5 and earlier 6.x versions; VMware Player 1.0.8 and earlier, and 2.0.5 and earlier 2.x versions; VMware Server 1.0.9 and earlier; VMware ESXi 3.5; and VMware ESX 3.0.2 through 3.5 allows guest OS users to have an unknown impact by sending the virtual hardware a request that triggers an arbitrary physical-memory write operation, leading to memory corruption.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	32597
CVE	CVE-2008-4917
OVAL	6246
URL	http://www.vmware.com/security/advisories/VMSA-2008-0019.html

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.9

Upgrade to VMware Player version 1.0.9

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player < 2.5.0

Upgrade to VMware Player version 2.5.0

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.43. VMware Workstation: Critical Memory corruption vulnerability (VMSA-2008-0019) (CVE-2008-4917) (vmsa-2008-0019-cve-2008-4917-workstation)

Description:

Unspecified vulnerability in VMware Workstation 5.5.8 and earlier, and 6.0.5 and earlier 6.x versions; VMware Player 1.0.8 and earlier, and 2.0.5 and earlier 2.x versions; VMware Server 1.0.9 and earlier; VMware ESXi 3.5; and VMware ESX 3.0.2 through 3.5 allows guest OS users to have an unknown impact by sending the virtual hardware a request that triggers an arbitrary physical-memory write operation, leading to memory corruption.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	32597
CVE	CVE-2008-4917
OVAL	6246
URL	http://www.vmware.com/security/advisories/VMSA-2008-0019.html

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.9

Upgrade to VMware Workstation version 5.5.9

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation < 6.5.0

Upgrade to VMware Workstation version 6.5.0

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

3.2.44. VMware Player: VNnc Codec Heap Overflow vulnerabilities (VMSA-2009-0005) (CVE-2009-0910) (vmsa-2009-0005-cve-2009-0910-player)

Description:

Heap-based buffer overflow in the VNnc Codec in VMware Workstation 6.5.x before 6.5.2 build 156735, VMware Player 2.5.x before 2.5.2 build 156735, VMware ACE 2.5.x before 2.5.2 build 156735, and VMware Server 2.0.x before 2.0.1 build 156745 allows remote attackers to execute arbitrary code via a crafted web page or video file, aka ZDI-CAN-436.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	34373
CVE	CVE-2009-0910
OVAL	5786
URL	http://www.vmware.com/security/advisories/VMSA-2009-0005.html

Vulnerability Solution:

VMware Player >= 2.5 and < 2.5.2
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.45. VMware Workstation: VNnc Codec Heap Overflow vulnerabilities (VMSA-2009-0005) (CVE-2009-0910) (vmsa-2009-0005-cve-2009-0910-workstation)

Description:

Heap-based buffer overflow in the VNnc Codec in VMware Workstation 6.5.x before 6.5.2 build 156735, VMware Player 2.5.x before 2.5.2 build 156735, VMware ACE 2.5.x before 2.5.2 build 156735, and VMware Server 2.0.x before 2.0.1 build 156745 allows remote attackers to execute arbitrary code via a crafted web page or video file, aka ZDI-CAN-436.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	34373
CVE	CVE-2009-0910
OVAL	5786

Source	Reference
URL	http://www.vmware.com/security/advisories/VMSA-2009-0005.html

Vulnerability Solution:

VMware Workstation >= 6.5 and < 6.5.2
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

3.2.46. VMware Player: Host code execution vulnerability from a guest operating system (VMSA-2009-0006) (CVE-2009-1244) (vmsa-2009-0006-cve-2009-1244-player)

Description:

Unspecified vulnerability in the virtual machine display function in VMware Workstation 6.5.1 and earlier; VMware Player 2.5.1 and earlier; VMware ACE 2.5.1 and earlier; VMware Server 1.x before 1.0.9 build 156507 and 2.x before 2.0.1 build 156745; VMware Fusion before 2.0.4 build 159196; VMware ESXi 3.5; and VMware ESX 3.0.2, 3.0.3, and 3.5 allows guest OS users to execute arbitrary code on the host OS via unknown vectors, a different vulnerability than CVE-2008-4916.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	34471
CVE	CVE-2009-1244
OVAL	6065
URL	http://www.vmware.com/security/advisories/VMSA-2009-0006.html
XF	49834

Vulnerability Solution:

VMware Player >= 2.5 and < 2.5.2
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.47. VMware Workstation: Host code execution vulnerability from a guest operating system (VMSA-2009-0006) (CVE-2009-1244) (vmsa-2009-0006-cve-2009-1244-workstation)

Description:

Unspecified vulnerability in the virtual machine display function in VMware Workstation 6.5.1 and earlier; VMware Player 2.5.1 and earlier; VMware ACE 2.5.1 and earlier; VMware Server 1.x before 1.0.9 build 156507 and 2.x before 2.0.1 build 156745; VMware Fusion before 2.0.4 build 159196; VMware ESXi 3.5; and VMware ESX 3.0.2, 3.0.3, and 3.5 allows guest OS users to execute arbitrary code on the host OS via unknown vectors, a different vulnerability than CVE-2008-4916.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	34471
CVE	CVE-2009-1244
OVAL	6065
URL	http://www.vmware.com/security/advisories/VMSA-2009-0006.html
XF	49834

Vulnerability Solution:

VMware Workstation >= 6.5 and < 6.5.2
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

3.2.48. VMware Player: Third Party Library libpng Updated to 1.2.35 (VMSA-2009-0010) (CVE-2009-0040) (vmsa-2009-0010-cve-2009-0040-player)

Description:

The PNG reference library (aka libpng) before 1.0.43, and 1.2.x before 1.2.35, as used in pngcrush and other applications, allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted PNG file that triggers a free of an uninitialized pointer in (1) the png_read_png function, (2) pCAL chunk handling, or (3) setup of 16-bit gamma tables.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

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-2009-08-05-1

Source	Reference
BID	33827
BID	33990
CERT	TA09-133A
CERT	TA09-218A
CERT-VN	649212
CVE	CVE-2009-0040
DEBIAN	DSA-1750
DEBIAN	DSA-1830
OVAL	10316
OVAL	6458
REDHAT	RHSA-2009:0315
REDHAT	RHSA-2009:0325
REDHAT	RHSA-2009:0333
REDHAT	RHSA-2009:0340
SUSE	SUSE-SA:2009:012
SUSE	SUSE-SA:2009:023
URL	http://www.vmware.com/security/advisories/VMSA-2009-0010.html
XF	48819

Vulnerability Solution:

VMware Player >= 2.5 and < 2.5.3
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.49. VMware Workstation: Third Party Library libpng Updated to 1.2.35 (VMSA-2009-0010) (CVE-2009-0040) (vmsa-2009-0010-cve-2009-0040-workstation)

Description:

The PNG reference library (aka libpng) before 1.0.43, and 1.2.x before 1.2.35, as used in pngcrush and other applications, allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted PNG file that triggers a free of an uninitialized pointer in (1) the png_read_png function, (2) pCAL chunk handling, or (3) setup of 16-bit gamma tables.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

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-2009-08-05-1
BID	33827
BID	33990
CERT	TA09-133A
CERT	TA09-218A
CERT-VN	649212
CVE	CVE-2009-0040
DEBIAN	DSA-1750
DEBIAN	DSA-1830
OVAL	10316
OVAL	6458
REDHAT	RHSA-2009:0315
REDHAT	RHSA-2009:0325
REDHAT	RHSA-2009:0333
REDHAT	RHSA-2009:0340
SUSE	SUSE-SA:2009:012
SUSE	SUSE-SA:2009:023
URL	http://www.vmware.com/security/advisories/VMSA-2009-0010.html
XF	48819

Vulnerability Solution:

VMware Workstation >= 6.5 and < 6.5.3
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

3.2.50. VMware Player: Mishandled exception on page faults (VMSA-2009-0015) (CVE-2009-2267) (vmsa-2009-0015-cve-2009-2267-player)

Description:

VMware Workstation 6.5.x before 6.5.3 build 185404, VMware Player 2.5.x before 2.5.3 build 185404, VMware ACE 2.5.x before 2.5.3 build 185404, VMware Server 1.x before 1.0.10 build 203137 and 2.x before 2.0.2 build 203138, VMware Fusion 2.x before 2.0.6 build 196839, VMware ESXi 3.5 and 4.0, and VMware ESX 2.5.5, 3.0.3, 3.5, and 4.0, when Virtual-8086 mode is used, do not properly set the exception code upon a page fault (aka #PF) exception, which allows guest OS users to gain privileges on the guest OS by

specifying a crafted value for the cs register.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	36841
CVE	CVE-2009-2267
OVAL	8473
URL	http://www.vmware.com/security/advisories/VMSA-2009-0015.html

Vulnerability Solution:

VMware Player >= 2.5 and < 2.5.3
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.51. VMware Workstation: Mishandled exception on page faults (VMSA-2009-0015) (CVE-2009-2267) (vmsa-2009-0015-cve-2009-2267-workstation)

Description:

VMware Workstation 6.5.x before 6.5.3 build 185404, VMware Player 2.5.x before 2.5.3 build 185404, VMware ACE 2.5.x before 2.5.3 build 185404, VMware Server 1.x before 1.0.10 build 203137 and 2.x before 2.0.2 build 203138, VMware Fusion 2.x before 2.0.6 build 196839, VMware ESXi 3.5 and 4.0, and VMware ESX 2.5.5, 3.0.3, 3.5, and 4.0, when Virtual-8086 mode is used, do not properly set the exception code upon a page fault (aka #PF) exception, which allows guest OS users to gain privileges on the guest OS by specifying a crafted value for the cs register.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	36841
CVE	CVE-2009-2267
OVAL	8473
URL	http://www.vmware.com/security/advisories/VMSA-2009-0015.html

Vulnerability Solution:

VMware Workstation >= 6.5 and < 6.5.3
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

3.2.52. VMware Player: Linux-based vmrun format string vulnerability (VMSA-2010-0007) (CVE-2010-1139) (vmsa-2010-0007-cve-2010-1139-player)

Description:

Format string vulnerability in vmrun in VMware VIX API 1.6.x, VMware Workstation 6.5.x before 6.5.4 build 246459, VMware Player 2.5.x before 2.5.4 build 246459, and VMware Server 2.x on Linux, and VMware Fusion 2.x before 2.0.7 build 246742, allows local users to gain privileges via format string specifiers in process metadata.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Player

References:

Source	Reference
BID	39407
CVE	CVE-2010-1139
DISA_SEVERITY	Category I
DISA_VMSKEY	V0023997
IAVM	2010-A-0066
URL	http://www.vmware.com/security/advisories/VMSA-2010-0007.html

Vulnerability Solution:

VMware Player >= 2.5 and < 2.5.4
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.53. VMware Workstation: Linux-based vmrun format string vulnerability (VMSA-2010-0007) (CVE-2010-1139) (vmsa-2010-0007-cve-2010-1139-workstation)

Description:

Format string vulnerability in vmrun in VMware VIX API 1.6.x, VMware Workstation 6.5.x before 6.5.4 build 246459, VMware Player 2.5.x before 2.5.4 build 246459, and VMware Server 2.x on Linux, and VMware Fusion 2.x before 2.0.7 build 246742, allows local users to gain privileges via format string specifiers in process metadata.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	39407
CVE	CVE-2010-1139
DISA_SEVERITY	Category I
DISA_VMSKEY	V0023997
IAVM	2010-A-0066
URL	http://www.vmware.com/security/advisories/VMSA-2010-0007.html

Vulnerability Solution:

VMware Workstation >= 6.5 and < 6.5.4
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

3.2.54. VMware Player: VMware Workstation, Player and Fusion vmware-mount race condition (VMSA-2010-0018) (CVE-2010-4295) (vmsa-2010-0018-cve-2010-4295-player)

Description:

Race condition in the mounting process in vmware-mount in VMware Workstation 7.x before 7.1.2 build 301548 on Linux, VMware Player 3.1.x before 3.1.2 build 301548 on Linux, VMware Server 2.0.2 on Linux, and VMware Fusion 3.1.x before 3.1.2 build 332101 allows host OS users to gain privileges via vectors involving temporary files.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Player

References:

Source	Reference
BID	45167
CVE	CVE-2010-4295
DISA_SEVERITY	Category II

Source	Reference
DISA_VMSKEY	V0025835
IAVM	2010-A-0168
URL	http://www.vmware.com/security/advisories/VMSA-2010-0018.html

Vulnerability Solution:

VMware Player >= 3.1 and < 3.1.2
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.55. VMware Workstation: VMware Workstation, Player and Fusion vmware-mount race condition (VMSA-2010-0018) (CVE-2010-4295) (vmsa-2010-0018-cve-2010-4295-workstation)

Description:

Race condition in the mounting process in vmware-mount in VMware Workstation 7.x before 7.1.2 build 301548 on Linux, VMware Player 3.1.x before 3.1.2 build 301548 on Linux, VMware Server 2.0.2 on Linux, and VMware Fusion 3.1.x before 3.1.2 build 332101 allows host OS users to gain privileges via vectors involving temporary files.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	45167
CVE	CVE-2010-4295
DISA_SEVERITY	Category II
DISA_VMSKEY	V0025835
IAVM	2010-A-0168
URL	http://www.vmware.com/security/advisories/VMSA-2010-0018.html

Vulnerability Solution:

VMware Workstation >= 7 and < 7.1.2
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.2.56. VMware Player: VMware Workstation, Player and Fusion vmware-mount privilegeb. VMware Workstation, Player and Fusion vmware-mount privilege (VMSA-2010-0018) (CVE-2010-4296) (vmsa-2010-0018-cve-2010-4296-player)

Description:

vmware-mount in VMware Workstation 7.x before 7.1.2 build 301548 on Linux, VMware Player 3.1.x before 3.1.2 build 301548 on Linux, VMware Server 2.0.2 on Linux, and VMware Fusion 3.1.x before 3.1.2 build 332101 does not properly load libraries, which allows host OS users to gain privileges via vectors involving shared object files.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Player

References:

Source	Reference
BID	45168
CVE	CVE-2010-4296
DISA_SEVERITY	Category II
DISA_VMSKEY	V0025835
IAVM	2010-A-0168
URL	http://www.vmware.com/security/advisories/VMSA-2010-0018.html

Vulnerability Solution:

VMware Player >= 3.1 and < 3.1.2
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.57. VMware Workstation: VMware Workstation, Player and Fusion vmware-mount privilegeb. VMware Workstation, Player and Fusion vmware-mount privilege (VMSA-2010-0018) (CVE-2010-4296) (vmsa-2010-0018-cve-2010-4296-workstation)

Description:

vmware-mount in VMware Workstation 7.x before 7.1.2 build 301548 on Linux, VMware Player 3.1.x before 3.1.2 build 301548 on Linux, VMware Server 2.0.2 on Linux, and VMware Fusion 3.1.x before 3.1.2 build 332101 does not properly load libraries, which allows host OS users to gain privileges via vectors involving shared object files.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	45168
CVE	CVE-2010-4296
DISA_SEVERITY	Category II
DISA_VMSKEY	V0025835
IAVM	2010-A-0168
URL	http://www.vmware.com/security/advisories/VMSA-2010-0018.html

Vulnerability Solution:

VMware Workstation >= 7 and < 7.1.2
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.2.58. VMware Player: OS Command Injection in VMware Tools update (VMSA-2010-0018) (CVE-2010-4297) (vmsa-2010-0018-cve-2010-4297-player)

Description:

The VMware Tools update functionality in VMware Workstation 6.5.x before 6.5.5 build 328052 and 7.x before 7.1.2 build 301548; VMware Player 2.5.x before 2.5.5 build 328052 and 3.1.x before 3.1.2 build 301548; VMware Server 2.0.2; VMware Fusion 2.x before 2.0.8 build 328035 and 3.1.x before 3.1.2 build 332101; VMware ESXi 3.5, 4.0, and 4.1; and VMware ESX 3.0.3, 3.5, 4.0, and 4.1 allows host OS users to gain privileges on the guest OS via unspecified vectors, related to a "command injection" issue.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	45166
CVE	CVE-2010-4297
DISA_SEVERITY	Category II
DISA_VMSKEY	V0025835
IAVM	2010-A-0168
URL	http://www.vmware.com/security/advisories/VMSA-2010-0018.html

Vulnerability Solution:

•VMware Player >= 2.5 and < 2.5.5
Upgrade to VMware Player version 2.5.5

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 3.1 and < 3.1.2

Upgrade to VMware Player version 3.1.2

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.59. VMware Workstation: OS Command Injection in VMware Tools update (VMSA-2010-0018) (CVE-2010-4297) (vmsa-2010-0018-cve-2010-4297-workstation)

Description:

The VMware Tools update functionality in VMware Workstation 6.5.x before 6.5.5 build 328052 and 7.x before 7.1.2 build 301548; VMware Player 2.5.x before 2.5.5 build 328052 and 3.1.x before 3.1.2 build 301548; VMware Server 2.0.2; VMware Fusion 2.x before 2.0.8 build 328035 and 3.1.x before 3.1.2 build 332101; VMware ESXi 3.5, 4.0, and 4.1; and VMware ESX 3.0.3, 3.5, 4.0, and 4.1 allows host OS users to gain privileges on the guest OS via unspecified vectors, related to a "command injection" issue.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	45166
CVE	CVE-2010-4297
DISA_SEVERITY	Category II
DISA_VMSKEY	V0025835
IAVM	2010-A-0168
URL	http://www.vmware.com/security/advisories/VMSA-2010-0018.html

Vulnerability Solution:

•VMware Workstation >= 6.5 and < 6.5.5

Upgrade to VMware Workstation version 6.5.5

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

•VMware Workstation >= 7 and < 7.1.2

Upgrade to VMware Workstation version 7.1.2

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.2.60. VMware Workstation: VMware Linux based vmrun utility local privilege escalation (VMSA-2011-0006) (CVE-2011-1126) (vmsa-2011-0006-cve-2011-1126-workstation)

Description:

VMware vmrun, as used in VIX API 1.x before 1.10.3 and VMware Workstation 6.5.x and 7.x before 7.1.4 build 385536 on Linux, might allow local users to gain privileges via a Trojan horse shared library in an unspecified directory.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	47094
CVE	CVE-2011-1126
URL	http://www.vmware.com/security/advisories/VMSA-2011-0006.html
XF	66472

Vulnerability Solution:

VMware Workstation >= 7 and < 7.1.4
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.2.61. VMware Player: Multiple vulnerabilities in mount.vmhgfs (VMSA-2011-0009) (CVE-2011-1787) (vmsa-2011-0009-cve-2011-1787-player)

Description:

Race condition in mount.vmhgfs in the VMware Host Guest File System (HGFS) in VMware Workstation 7.1.x before 7.1.4, VMware Player 3.1.x before 3.1.4, VMware Fusion 3.1.x before 3.1.3, VMware ESXi 3.5 through 4.1, and VMware ESX 3.0.3 through 4.1 allows guest OS users to gain privileges on the guest OS by mounting a filesystem on top of an arbitrary directory.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Player

References:

Source	Reference
BID	48098

Source	Reference
CVE	CVE-2011-1787
DISA_SEVERITY	Category I
DISA_VMSKEY	V0028311
IAVM	2011-A-0075
URL	http://www.vmware.com/security/advisories/VMSA-2011-0009.html

Vulnerability Solution:

VMware Player >= 3.1 and < 3.1.4
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.62. VMware Workstation: Multiple vulnerabilities in mount.vmhgfs (VMSA-2011-0009) (CVE-2011-1787) (vmsa-2011-0009-cve-2011-1787-workstation)

Description:

Race condition in mount.vmhgfs in the VMware Host Guest File System (HGFS) in VMware Workstation 7.1.x before 7.1.4, VMware Player 3.1.x before 3.1.4, VMware Fusion 3.1.x before 3.1.3, VMware ESXi 3.5 through 4.1, and VMware ESX 3.0.3 through 4.1 allows guest OS users to gain privileges on the guest OS by mounting a filesystem on top of an arbitrary directory.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	48098
CVE	CVE-2011-1787
DISA_SEVERITY	Category I
DISA_VMSKEY	V0028311
IAVM	2011-A-0075
URL	http://www.vmware.com/security/advisories/VMSA-2011-0009.html

Vulnerability Solution:

VMware Workstation >= 7 and < 7.1.4
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.2.63. VMware Player: VMware Tools Display Driver Privilege Escalation (XPDM null pointer dereference) (VMSA-2012-0005) (CVE-2012-1508) (vmsa-2012-0005-cve-2012-1508-player)

Description:

The XPDM display driver in VMware ESXi 4.0, 4.1, and 5.0; VMware ESX 4.0 and 4.1; and VMware View before 4.6.1 allows guest OS users to gain guest OS privileges or cause a denial of service (NULL pointer dereference) via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	52524
CVE	CVE-2012-1508
DISA_SEVERITY	Category I
DISA_VMSKEY	V0031898
DISA_VMSKEY	V0031899
IAVM	2012-A-0045
IAVM	2012-A-0046
OVAL	17183
URL	http://www.vmware.com/security/advisories/VMSA-2012-0005.html

Vulnerability Solution:

VMware Player >= 3.1 and < 3.1.4
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.64. VMware Workstation: VMware Tools Display Driver Privilege Escalation (XPDM null pointer dereference) (VMSA-2012-0005) (CVE-2012-1508) (vmsa-2012-0005-cve-2012-1508-workstation)

Description:

The XPDM display driver in VMware ESXi 4.0, 4.1, and 5.0; VMware ESX 4.0 and 4.1; and VMware View before 4.6.1 allows guest OS users to gain guest OS privileges or cause a denial of service (NULL pointer dereference) via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	52524
CVE	CVE-2012-1508
DISA_SEVERITY	Category I
DISA_VMSKEY	V0031898
DISA_VMSKEY	V0031899
IAVM	2012-A-0045
IAVM	2012-A-0046
OVAL	17183
URL	http://www.vmware.com/security/advisories/VMSA-2012-0005.html

Vulnerability Solution:

VMware Workstation >= 7 and < 7.1.4
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.2.65. VMware Player: VMware Tools Display Driver Privilege Escalation (XPDM buffer overrun) (VMSA-2012-0005) (CVE-2012-1509) (vmsa-2012-0005-cve-2012-1509-player)

Description:

Buffer overflow in the XPDM display driver in VMware View before 4.6.1 allows guest OS users to gain guest OS privileges via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	52524
CVE	CVE-2012-1509
OVAL	17151
URL	http://www.vmware.com/security/advisories/VMSA-2012-0005.html
XF	74096

Vulnerability Solution:

VMware Player >= 3.1 and < 3.1.4
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.66. VMware Workstation: VMware Tools Display Driver Privilege Escalation (XPDM buffer overrun) (VMSA-2012-0005) (CVE-2012-1509) (vmsa-2012-0005-cve-2012-1509-workstation)

Description:

Buffer overflow in the XPDM display driver in VMware View before 4.6.1 allows guest OS users to gain guest OS privileges via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	52524
CVE	CVE-2012-1509
OVAL	17151
URL	http://www.vmware.com/security/advisories/VMSA-2012-0005.html
XF	74096

Vulnerability Solution:

VMware Workstation >= 7 and < 7.1.4
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.2.67. VMware Player: VMware Tools Display Driver Privilege Escalation (WDDM buffer overrun) (VMSA-2012-0005) (CVE-2012-1510) (vmsa-2012-0005-cve-2012-1510-player)

Description:

Buffer overflow in the WDDM display driver in VMware ESXi 4.0, 4.1, and 5.0; VMware ESX 4.0 and 4.1; and VMware View before 4.6.1 allows guest OS users to gain guest OS privileges via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	52524

Source	Reference
CVE	CVE-2012-1510
DISA_SEVERITY	Category I
DISA_VMSKEY	V0031898
DISA_VMSKEY	V0031899
IAVM	2012-A-0045
IAVM	2012-A-0046
OVAL	17258
URL	http://www.vmware.com/security/advisories/VMSA-2012-0005.html
XF	74097

Vulnerability Solution:

VMware Player >= 3.1 and < 3.1.4
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.68. VMware Workstation: VMware Tools Display Driver Privilege Escalation (WDDM buffer overrun) (VMSA-2012-0005) (CVE-2012-1510) (vmsa-2012-0005-cve-2012-1510-workstation)

Description:

Buffer overflow in the WDDM display driver in VMware ESXi 4.0, 4.1, and 5.0; VMware ESX 4.0 and 4.1; and VMware View before 4.6.1 allows guest OS users to gain guest OS privileges via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	52524
CVE	CVE-2012-1510
DISA_SEVERITY	Category I
DISA_VMSKEY	V0031898
DISA_VMSKEY	V0031899
IAVM	2012-A-0045
IAVM	2012-A-0046
OVAL	17258

Source	Reference
URL	http://www.vmware.com/security/advisories/VMSA-2012-0005.html
XF	74097

Vulnerability Solution:

VMware Workstation >= 7 and < 7.1.4
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.2.69. VMware Player: VMware shared library privilege escalation (VMSA-2013-0013) (CVE-2013-5972) (vmsa-2013-0013-cve-2013-5972-player)

Description:

VMware Workstation 9.x before 9.0.3 and VMware Player 5.x before 5.0.3 on Linux do not properly handle shared libraries, which allows host OS users to gain host OS privileges via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Player

References:

Source	Reference
CVE	CVE-2013-5972
URL	http://www.vmware.com/security/advisories/VMSA-2013-0013.html

Vulnerability Solution:

VMware Player >= 5.0 and < 5.0.3
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.70. VMware Workstation: VMware shared library privilege escalation (VMSA-2013-0013) (CVE-2013-5972) (vmsa-2013-0013-cve-2013-5972-workstation)

Description:

VMware Workstation 9.x before 9.0.3 and VMware Player 5.x before 5.0.3 on Linux do not properly handle shared libraries, which allows host OS users to gain host OS privileges via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Workstation

References:

Source	Reference
CVE	CVE-2013-5972
URL	http://www.vmware.com/security/advisories/VMSA-2013-0013.html

Vulnerability Solution:

VMware Workstation >= 9 and < 9.0.3
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/9_0

3.2.71. VMware Player: OpenSSL update for multiple products (VMSA-2014-0006) (CVE-2014-0195) (vmsa-2014-0006-cve-2014-0195-player)

Description:

The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	67900
CVE	CVE-2014-0195
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052641
IAVM	2014-B-0077
IAVM	2014-B-0079
URL	http://www.vmware.com/security/advisories/VMSA-2014-0006.html

Vulnerability Solution:

•VMware Player >= 5.0 and < 5.0.4

Upgrade to VMware Player version 5.0.4

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 6.0 and < 6.0.3

Upgrade to VMware Player version 6.0.3

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.72. VMware Workstation: OpenSSL update for multiple products (VMSA-2014-0006) (CVE-2014-0195) (vmsa-2014-0006-cve-2014-0195-workstation)

Description:

The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	67900
CVE	CVE-2014-0195
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052641
IAVM	2014-B-0077
IAVM	2014-B-0079
URL	http://www.vmware.com/security/advisories/VMSA-2014-0006.html

Vulnerability Solution:

•VMware Workstation >= 10 and < 10.0.3

Upgrade to VMware Workstation version 10.0.3

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

•VMware Workstation >= 9 and < 9.0.4

Upgrade to VMware Workstation version 9.0.4

Download and apply the upgrade from:

https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/9_0

3.2.73. VMware Player: OpenSSL update for multiple products (VMSA-2014-0006) (CVE-2014-0224) (vmsa-2014-0006-cve-2014-0224-player)

Description:

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
CERT-VN	978508
CVE	CVE-2014-0224
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052641
DISA_VMSKEY	V0052893
DISA_VMSKEY	V0052901
DISA_VMSKEY	V0052907
DISA_VMSKEY	V0052909
DISA_VMSKEY	V0052911
DISA_VMSKEY	V0053319
DISA_VMSKEY	V0053501
DISA_VMSKEY	V0053505
DISA_VMSKEY	V0053507
DISA_VMSKEY	V0060737
IAVM	2014-A-0115
IAVM	2014-B-0077
IAVM	2014-B-0079

Source	Reference
IAVM	2014-B-0084
IAVM	2014-B-0088
IAVM	2014-B-0089
IAVM	2014-B-0091
IAVM	2014-B-0092
IAVM	2014-B-0097
IAVM	2014-B-0101
IAVM	2014-B-0102
IAVM	2015-A-0113
REDHAT	RHSA-2014:0624
REDHAT	RHSA-2014:0626
REDHAT	RHSA-2014:0627
REDHAT	RHSA-2014:0630
REDHAT	RHSA-2014:0631
REDHAT	RHSA-2014:0632
REDHAT	RHSA-2014:0633
REDHAT	RHSA-2014:0680
URL	http://www.vmware.com/security/advisories/VMSA-2014-0006.html

Vulnerability Solution:

•VMware Player >= 5.0 and < 5.0.4

Upgrade to VMware Player version 5.0.4

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 6.0 and < 6.0.3

Upgrade to VMware Player version 6.0.3

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.74. VMware Workstation: OpenSSL update for multiple products (VMSA-2014-0006) (CVE-2014-0224) (vmsa-2014-0006-cve-2014-0224-workstation)

Description:

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
CERT-VN	978508
CVE	CVE-2014-0224
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052641
DISA_VMSKEY	V0052893
DISA_VMSKEY	V0052901
DISA_VMSKEY	V0052907
DISA_VMSKEY	V0052909
DISA_VMSKEY	V0052911
DISA_VMSKEY	V0053319
DISA_VMSKEY	V0053501
DISA_VMSKEY	V0053505
DISA_VMSKEY	V0053507
DISA_VMSKEY	V0060737
IAVM	2014-A-0115
IAVM	2014-B-0077
IAVM	2014-B-0079
IAVM	2014-B-0084
IAVM	2014-B-0088
IAVM	2014-B-0089
IAVM	2014-B-0091
IAVM	2014-B-0092
IAVM	2014-B-0097
IAVM	2014-B-0101
IAVM	2014-B-0102
IAVM	2015-A-0113
REDHAT	RHSA-2014:0624

Source	Reference
REDHAT	RHSA-2014:0626
REDHAT	RHSA-2014:0627
REDHAT	RHSA-2014:0630
REDHAT	RHSA-2014:0631
REDHAT	RHSA-2014:0632
REDHAT	RHSA-2014:0633
REDHAT	RHSA-2014:0680
URL	http://www.vmware.com/security/advisories/VMSA-2014-0006.html

Vulnerability Solution:

•VMware Workstation >= 10 and < 10.0.3

Upgrade to VMware Workstation version 10.0.3

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

•VMware Workstation >= 9 and < 9.0.4

Upgrade to VMware Workstation version 9.0.4

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/9_0

3.2.75. VMware Player: Vulnerability (VMSA-2015-0004) (CVE-2012-0897) (vmsa-2015-0004-cve-2012-0897-player)

Description:

Stack-based buffer overflow in the JPEG2000 plugin in IrfanView PlugIns before 4.33 allows remote attackers to execute arbitrary code via a JPEG2000 (JP2) file with a crafted Quantization Default (QCD) marker segment.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	51426
CVE	CVE-2012-0897
DISA_SEVERITY	Category I
DISA_VMSKEY	V0060965
IAVM	2015-B-0076

Source	Reference
URL	http://www.vmware.com/security/advisories/VMSA-2015-0004.html
XF	72398

Vulnerability Solution:

VMware Player >= 6.0 and < 6.0.6
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.76. VMware Workstation: Vulnerability (VMSA-2015-0004) (CVE-2012-0897) (vmsa-2015-0004-cve-2012-0897-workstation)

Description:

Stack-based buffer overflow in the JPEG2000 plugin in IrfanView PlugIns before 4.33 allows remote attackers to execute arbitrary code via a JPEG2000 (JP2) file with a crafted Quantization Default (QCD) marker segment.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	51426
CVE	CVE-2012-0897
DISA_SEVERITY	Category I
DISA_VMSKEY	V0060965
IAVM	2015-B-0076
URL	http://www.vmware.com/security/advisories/VMSA-2015-0004.html
XF	72398

Vulnerability Solution:

VMware Workstation >= 10 and < 10.0.5
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

3.2.77. VMware Player: Vulnerability (VMSA-2016-0001) (CVE-2015-6933) (vmsa-2016-0001-cve-2015-6933-player)

Description:

The VMware Tools HGFS (aka Shared Folders) implementation in VMware Workstation 11.x before 11.1.2, VMware Player 7.x before 7.1.2, VMware Fusion 7.x before 7.1.2, and VMware ESXi 5.0 through 6.0 allows Windows guest OS users to gain guest OS privileges or cause a denial of service (guest OS kernel memory corruption) via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
CVE	CVE-2015-6933
DISA_SEVERITY	Category II
IAVM	2016-B-0013
IAVM	2016-B-0014
IAVM	2016-B-0015
IAVM	2016-B-0016
URL	http://www.vmware.com/security/advisories/VMSA-2016-0001.html

Vulnerability Solution:

VMware Player >= 7.1 and < 7.1.2
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.78. VMware Workstation: Vulnerability (VMSA-2016-0001) (CVE-2015-6933) (vmsa-2016-0001-cve-2015-6933-workstation)

Description:

The VMware Tools HGFS (aka Shared Folders) implementation in VMware Workstation 11.x before 11.1.2, VMware Player 7.x before 7.1.2, VMware Fusion 7.x before 7.1.2, and VMware ESXi 5.0 through 6.0 allows Windows guest OS users to gain guest OS privileges or cause a denial of service (guest OS kernel memory corruption) via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
CVE	CVE-2015-6933
DISA_SEVERITY	Category II
IAVM	2016-B-0013

Source	Reference
IAVM	2016-B-0014
IAVM	2016-B-0015
IAVM	2016-B-0016
URL	http://www.vmware.com/security/advisories/VMSA-2016-0001.html

Vulnerability Solution:

VMware Workstation >= 11 and < 11.1.2
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/11_0

3.2.79. VMware Player: VMware Workstation and Fusion out-of-bounds memory access vulnerability (VMSA-2016-0019) (CVE-2016-7461) (vmsa-2016-0019-cve-2016-7461-player)

Description:

The drag-and-drop (aka DnD) function in VMware Workstation Pro 12.x before 12.5.2 and VMware Workstation Player 12.x before 12.5.2 and VMware Fusion and Fusion Pro 8.x before 8.5.2 allows guest OS users to execute arbitrary code on the host OS or cause a denial of service (out-of-bounds memory access on the host OS) via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	94280
CVE	CVE-2016-7461
DISA_SEVERITY	Category I
IAVM	2016-A-0326
IAVM	2016-B-0165
URL	http://www.vmware.com/security/advisories/VMSA-2016-0019.html

Vulnerability Solution:

VMware Player >= 12.5 and < 12.5.2
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.80. VMware Workstation: VMware Workstation and Fusion out-of-bounds memory access vulnerability (VMSA-2016-0019) (CVE-2016-7461) (vmsa-2016-0019-cve-2016-7461-workstation)

Description:

The drag-and-drop (aka DnD) function in VMware Workstation Pro 12.x before 12.5.2 and VMware Workstation Player 12.x before 12.5.2 and VMware Fusion and Fusion Pro 8.x before 8.5.2 allows guest OS users to execute arbitrary code on the host OS or cause a denial of service (out-of-bounds memory access on the host OS) via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	94280
CVE	CVE-2016-7461
DISA_SEVERITY	Category I
IAVM	2016-A-0326
IAVM	2016-B-0165
URL	http://www.vmware.com/security/advisories/VMSA-2016-0019.html

Vulnerability Solution:

VMware Workstation >= 12.5 and < 12.5.2
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

3.2.81. VMware Workstation: Vulnerability (VMSA-2017-0006) (CVE-2017-4902) (vmsa-2017-0006-cve-2017-4902-workstation)

Description:

VMware ESXi 6.5 without patch ESXi650-201703410-SG and 5.5 without patch ESXi550-201703401-SG; Workstation Pro / Player 12.x prior to 12.5.5; and Fusion Pro / Fusion 8.x prior to 8.5.6 have a Heap Buffer Overflow in SVGA. This issue may allow a guest to execute code on the host.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference

Source	Reference
BID	97163
CVE	CVE-2017-4902
URL	http://www.vmware.com/security/advisories/VMSA-2017-0006.html

Vulnerability Solution:

VMware Workstation >= 12.5 and < 12.5.5
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

3.2.82. VMware Workstation: Vulnerability (VMSA-2017-0006) (CVE-2017-4903) (vmsa-2017-0006-cve-2017-4903-workstation)

Description:

VMware ESXi 6.5 without patch ESXi650-201703410-SG, 6.0 U3 without patch ESXi600-201703401-SG, 6.0 U2 without patch ESXi600-201703403-SG, 6.0 U1 without patch ESXi600-201703402-SG, and 5.5 without patch ESXi550-201703401-SG; Workstation Pro / Player 12.x prior to 12.5.5; and Fusion Pro / Fusion 8.x prior to 8.5.6 have an uninitialized stack memory usage in SVGA. This issue may allow a guest to execute code on the host.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	97160
CVE	CVE-2017-4903
URL	http://www.vmware.com/security/advisories/VMSA-2017-0006.html

Vulnerability Solution:

VMware Workstation >= 12.5 and < 12.5.5
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

3.2.83. VMware Workstation: Vulnerability (VMSA-2017-0006) (CVE-2017-4904) (vmsa-2017-0006-cve-2017-4904-workstation)

Description:

The XHCI controller in VMware ESXi 6.5 without patch ESXi650-201703410-SG, 6.0 U3 without patch ESXi600-201703401-SG, 6.0 U2 without patch ESXi600-201703403-SG, 6.0 U1 without patch ESXi600-201703402-SG, and 5.5 without patch ESXi550-201703401-SG; Workstation Pro / Player 12.x prior to 12.5.5; and Fusion Pro / Fusion 8.x prior to 8.5.6 has uninitialized memory usage. This issue may

allow a guest to execute code on the host. The issue is reduced to a Denial of Service of the guest on ESXi 5.5.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	97165
CVE	CVE-2017-4904
URL	http://www.vmware.com/security/advisories/VMSA-2017-0006.html

Vulnerability Solution:

VMware Workstation >= 12.5 and < 12.5.5
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

3.2.84. VMware Player: Vulnerability (VMSA-2017-0009) (CVE-2017-4915) (vmsa-2017-0009-cve-2017-4915-player)

Description:

VMware Workstation Pro/Player contains an insecure library loading vulnerability via ALSA sound driver configuration files. Successful exploitation of this issue may allow unprivileged host users to escalate their privileges to root in a Linux host machine.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Player

References:

Source	Reference
BID	98566
CVE	CVE-2017-4915
URL	http://www.vmware.com/security/advisories/VMSA-2017-0009.html

Vulnerability Solution:

VMware Player >= 12.5 and < 12.5.6
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.85. VMware Workstation: Vulnerability (VMSA-2017-0009) (CVE-2017-4915) (vmsa-2017-0009-cve-2017-4915-workstation)

Description:

VMware Workstation Pro/Player contains an insecure library loading vulnerability via ALSA sound driver configuration files. Successful exploitation of this issue may allow unprivileged host users to escalate their privileges to root in a Linux host machine.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	98566
CVE	CVE-2017-4915
URL	http://www.vmware.com/security/advisories/VMSA-2017-0009.html

Vulnerability Solution:

VMware Workstation >= 12.5 and < 12.5.6
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

3.2.86. VMware Workstation: Vulnerability (VMSA-2017-0015) (CVE-2017-4924) (vmsa-2017-0015-cve-2017-4924-workstation)

Description:

VMware ESXi (ESXi 6.5 without patch ESXi650-201707101-SG), Workstation (12.x before 12.5.7) and Fusion (8.x before 8.5.8) contain an out-of-bounds write vulnerability in SVGA device. This issue may allow a guest to execute code on the host.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	100843

Source	Reference
CVE	CVE-2017-4924
URL	http://www.vmware.com/security/advisories/VMSA-2017-0015.html

Vulnerability Solution:

VMware Workstation >= 12.5 and < 12.5.7
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

3.2.87. VMware Workstation: VMware Workstation, Fusion and Horizon View Client updates address heap buffer-overflow vulnerability (VMSA-2017-0018) (CVE-2017-4934) (vmsa-2017-0018-cve-2017-4934-workstation)

Description:

VMware Workstation (12.x before 12.5.8) and Fusion (8.x before 8.5.9) contain a heap buffer-overflow vulnerability in VMNAT device. This issue may allow a guest to execute code on the host.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	101903
CVE	CVE-2017-4934
URL	http://www.vmware.com/security/advisories/VMSA-2017-0018.html

Vulnerability Solution:

VMware Workstation >= 12.5 and < 12.5.8
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

3.2.88. VMware Workstation: Out-of-bounds read issue via Cortado ThinPrint (VMSA-2018-0003) (CVE-2017-4948) (vmsa-2018-0003-cve-2017-4948-workstation)

Description:

VMware Workstation (14.x before 14.1.0 and 12.x) and Horizon View Client (4.x before 4.7.0) contain an out-of-bounds read vulnerability in TPView.dll. On Workstation, this issue in conjunction with other bugs may allow a guest to leak information from host or may allow for a Denial of Service on the Windows OS that runs Workstation. In the case of a Horizon View Client, this issue in conjunction with other bugs may allow a View desktop to leak information from host or may allow for a Denial of Service on the Windows OS that runs the Horizon View Client. Exploitation is only possible if virtual printing has been enabled. This feature is not enabled by default on Workstation but it is enabled by default on Horizon View.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	102441
CVE	CVE-2017-4948
URL	http://www.vmware.com/security/advisories/VMSA-2018-0003.html

Vulnerability Solution:

VMware Workstation < 14.1.0
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/14_0

3.2.89. VMware Workstation: Vulnerability (VMSA-2018-0005) (CVE-2017-4949) (vmsa-2018-0005-cve-2017-4949-workstation)

Description:

VMware Workstation and Fusion contain a use-after-free vulnerability in VMware NAT service when IPv6 mode is enabled. This issue may allow a guest to execute code on the host. Note: IPv6 mode for VMNAT is not enabled by default.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	102489
CVE	CVE-2017-4949
URL	http://www.vmware.com/security/advisories/VMSA-2018-0005.html

Vulnerability Solution:

•VMware Workstation >= 12.5 and < 12.5.9

Upgrade to VMware Workstation version 12.5.9

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

•VMware Workstation >= 14 and < 14.1.1

Upgrade to VMware Workstation version 14.1.1

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/14_0

3.2.90. VMware Workstation: Vulnerability (VMSA-2018-0005) (CVE-2017-4950) (vmsa-2018-0005-cve-2017-4950-workstation)

Description:

VMware Workstation and Fusion contain an integer overflow vulnerability in VMware NAT service when IPv6 mode is enabled. This issue may lead to an out-of-bound read which can then be used to execute code on the host in conjunction with other issues. Note: IPv6 mode for VMNAT is not enabled by default.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	102490
CVE	CVE-2017-4950
URL	http://www.vmware.com/security/advisories/VMSA-2018-0005.html

Vulnerability Solution:

•VMware Workstation >= 12.5 and < 12.5.9

Upgrade to VMware Workstation version 12.5.9

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

•VMware Workstation >= 14 and < 14.1.1

Upgrade to VMware Workstation version 14.1.1

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/14_0

3.2.91. Apache HTTPD: APR-util off-by-one overflow (CVE-2009-1956) (apache-httpd-cve-2009-1956)

Description:

The affected asset is vulnerable to this vulnerability ONLY if an attacker can provide a specially crafted string to a function that handles a variable list of arguments on big-endian platforms. Review your web server configuration for validation. An off-by-one overflow flaw was found in the way the bundled copy of the APR-util library processed a variable list of arguments. An attacker could provide a specially-crafted string as input for the formatted output conversion routine, which could, on big-endian platforms, potentially lead to the

disclosure of sensitive information or a denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2009-11-09-1
BID	35251
CVE	CVE-2009-1956
OVAL	11567
OVAL	12237
REDHAT	RHSA-2009:1107
REDHAT	RHSA-2009:1108
URL	http://httpd.apache.org/security/vulnerabilities_22.html

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.

3.2.92. 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:
192.168.234.131:80	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
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.

3.2.93. Samba MS-RPC Shell Command Injection Vulnerability (cifs-samba-shell-command-injection-vuln)

Description:

The MS-RPC functionality in smbd in Samba 3.0.0 through 3.0.25rc3 allows remote attackers to execute arbitrary commands via shell metacharacters involving the (1) SamrChangePassword function, when the "username map script" smb.conf option is enabled, and allows remote authenticated users to execute commands via shell metacharacters involving other MS-RPC functions in the (2) remote printer and (3) file share management.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:139	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian
192.168.234.131:445	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-2007-07-31
BID	23972
BID	25159
CERT-VN	268336
CVE	CVE-2007-2447
DEBIAN	DSA-1291
OVAL	10062
REDHAT	RHSA-2007:0354
SUSE	SUSE-SA:2007:031
URL	http://www.samba.org/samba/security/CVE-2007-2447.html

Vulnerability Solution:

Samba < 3.0.25
Download and apply the upgrade from: https://ftp.samba.org/pub/samba/stable/samba-3.0.25.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.

3.2.94. 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:
192.168.234.131	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.

3.2.95. SMB signing not required (cifs-smb-signing-not-required)

Description:

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

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:139	Smb signing is: disabled
192.168.234.130:445	Smb signing is: disabled
192.168.234.131:139	Smb signing is: disabled
192.168.234.131:445	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

3.2.96. SMBv2 signing not required (cifs-smb2-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 2.x signing can be configured in one of two ways: not required (least secure) and required (most secure).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:445	Running CIFS serviceConfiguration item smb2-enabled set to 'true' matched Configuration item smb2-signing set to 'enabled' matched

References:

Source	Reference
URL	https://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

3.2.97. 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:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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	45137
CERT-VN	837744
CVE	CVE-2010-3614
DEBIAN	DSA-2130
REDHAT	RHSA-2010:0975
REDHAT	RHSA-2010:0976

Source	Reference
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.

3.2.98. 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:
192.168.234.130:80	Running HTTP serviceHTTP TRACE request to http://192.168.234.130/ 1: TRACE / HTTP/1.1 2: Host: 192.168.234.130 3: Cookie: vulnerable=yes
192.168.234.130:443	Running HTTPS serviceHTTP TRACE request to https://192.168.234.130/ 1: TRACE / HTTP/1.1 2: Host: 192.168.234.130:443 3: Cookie: vulnerable=yes
192.168.234.131:80	Running HTTP serviceHTTP TRACE request to http://192.168.234.131/ 1: TRACE / HTTP/1.1 2: Host: 192.168.234.131 3: Cookie: vulnerable=yes

References:

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

Source	Reference
CERT-VN	867593
CVE	CVE-2004-2320
CVE	CVE-2004-2763
CVE	CVE-2005-3398
CVE	CVE-2006-4683
CVE	CVE-2007-3008
CVE	CVE-2008-7253
CVE	CVE-2009-2823
CVE	CVE-2010-0386
DISA_SEVERITY	Category II
DISA_VMSKEY	V0011706
IAVM	2005-T-0043
OSVDB	35511
OSVDB	3726
OVAL	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".

3.2.99. MySQL Bug #29801: Remote Federated Engine Crash (mysql-bug-29801-remote-federated-engine-crash)

Description:

Versions of MySQL server before 5.0.52 and 5.1.23 suffer from a denial of service vulnerability via a flaw in the federated engine. On issuance of a command to a remote server (e.g., SHOW TABLE STATUS LIKE 'table'), the local federated server expects a query to contain fourteen columns. A response with less than fourteen columns causes the federated server to crash.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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.

3.2.100. MySQL Bug #32707: send_error() Buffer Overflow Vulnerability (mysql-bug-32707-send-error-bof)

Description:

A buffer overflow in MySQL 5.0 through 5.0.54 and 5.1 before 5.1.23 contains a flaw in the protocol layer. A long error message can cause a buffer overflow, potentially leading to execution of code.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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.

3.2.101. MySQL Bug #37428: User-Defind Function Remote Code Execution (mysql-bug-37428-user-defind-function-remote-codex)

Description:

MySQL server 5.0 before 5.0.67 contains a flaw in creating and dropping certain functions. Using MySQL's user-defined functions, an authenticated attacker can create a function in a shared library and run arbitrary code against the server.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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.

3.2.102. MySQL Bug #38296: Nested Boolean Query Exhaustion Denial of Service (mysql-bug-38296-nested-boolean-query-exhaustion-dos)

Description:

There is a flaw in parsing queries in MySQL 5.0 before 5.0.68 and MySQL 5.1 before 5.1.28. An attacker can potentially cause the server to crash by sending a query with multiple nested logic operators, e.g. 'SELECT * FROM TABLE WHERE ... OR (... OR (... OR (...' etc.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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.

3.2.103. MySQL COM_FIELD_LIST Command Buffer Overflow Vulnerability (mysql-com_field_list-command-bof)

Description:

Buffer overflow in MySQL 5.0 through 5.0.91 and 5.1 before 5.1.47 allows remote authenticated users to execute arbitrary code via a COM_FIELD_LIST command with a long table name.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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-2010-11-10-1
CVE	CVE-2010-1850
OVAL	10846
OVAL	6693
REDHAT	RHSA-2010:0442
URL	http://bugs.mysql.com/bug.php?id=53237
URL	http://dev.mysql.com/doc/refman/5.0/en/news-5-0-91.html
URL	http://dev.mysql.com/doc/refman/5.1/en/news-5-1-47.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.91

Upgrade to Oracle MySQL version 5.0.91

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 < 5.1.47

Upgrade to Oracle MySQL version 5.1.47

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.

3.2.104. Oracle MySQL Vulnerability: CVE-2012-0113 (oracle-mysql-cve-2012-0113)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect confidentiality and availability via unknown vectors, a different vulnerability than CVE-2012-0118.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0113
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.2.105. PHP Vulnerability: CVE-2008-3659 (php-cve-2008-3659)

Description:

Buffer overflow in the memnstr function in PHP 4.4.x before 4.4.9 and PHP 5.6 through 5.2.6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via the delimiter argument to the explode function. NOTE: the scope of this issue is limited since most applications would not use an attacker-controlled delimiter, but local attacks against safe_mode are feasible.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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
CERT	TA09-133A
CVE	CVE-2008-3659
DEBIAN	DSA-1647
XF	44405

Vulnerability Solution:

•Upgrade to PHP version 4.4.9

Download and apply the upgrade from: http://museum.php.net/php4/php-4.4.9.tar.gz

•Upgrade to PHP version 5.2.7

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

3.2.106. PHP Vulnerability: CVE-2010-1128 (php-cve-2010-1128)

Description:

The Linear Congruential Generator (LCG) in PHP before 5.2.13 does not provide the expected entropy, which makes it easier for context-dependent attackers to guess values that were intended to be unpredictable, as demonstrated by session cookies generated by using the uniqid function.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	38430
CVE	CVE-2010-1128
REDHAT	RHSA-2010:0919
URL	http://www.php.net/releases/5_2_13.php

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.13.tar.gz

3.2.107. PHP Vulnerability: CVE-2011-2202 (php-cve-2011-2202)

Description:

The rfc1867_post_handler function in main/rfc1867.c in PHP before 5.3.7 does not properly restrict filenames in multipart/form-data POST requests, which allows remote attackers to conduct absolute path traversal attacks, and possibly create or overwrite arbitrary files, via a crafted upload request, related to a "file path injection vulnerability."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2012-02-01-1
BID	48259
BID	49241
CVE	CVE-2011-2202
DEBIAN	DSA-2266
REDHAT	RHSA-2011:1423
REDHAT	RHSA-2012:0071
XF	67999

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

3.2.108. PHP Vulnerability: CVE-2012-0057 (php-cve-2012-0057)

Description:

PHP before 5.3.9 has improper libxslt security settings, which allows remote attackers to create arbitrary files via a crafted XSLT stylesheet that uses the libxslt output extension.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2012-0057
DEBIAN	DSA-2399
URL	https://bugs.php.net/bug.php?id=54446
XF	72908

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

3.2.109. PHP Vulnerability: CVE-2015-3411 (php-cve-2015-3411)

Description:

PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read or write to arbitrary files via crafted input to an application that calls (1) a DOMDocument load method, (2) the xmlwriter_open_uri function, (3) the finfo_file function, or (4) the hash_hmac_file function, as demonstrated by a filename\0.xml attack that bypasses an intended configuration in which client users may read only .xml files.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	75255
CVE	CVE-2015-3411
REDHAT	RHSA-2015:1135
REDHAT	RHSA-2015:1186
REDHAT	RHSA-2015:1187
REDHAT	RHSA-2015:1218

Vulnerability Solution:

•Upgrade to PHP version 5.4.40

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

•Upgrade to PHP version 5.5.24

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

•Upgrade to PHP version 5.6.8

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

3.2.110. PHP Vulnerability: CVE-2016-3185 (php-cve-2016-3185)

Description:

The make_http_soap_request function in ext/soap/php_http.c in PHP before 5.4.44, 5.5.x before 5.5.28, 5.6.x before 5.6.12, and 7.x before 7.0.4 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (type confusion and application crash) via crafted serialized _cookies data, related to the SoapClient::__call method in ext/soap/soap.c.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	84307
CVE	CVE-2016-3185

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/

•Upgrade to PHP version 7.0.4

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

3.2.111. PHP Vulnerability: CVE-2017-11147 (php-cve-2017-11147)

Description:

In PHP before 5.6.30 and 7.x before 7.0.15, the PHAR archive handler could be used by attackers supplying malicious archive files to crash the PHP interpreter or potentially disclose information due to a buffer over-read in the phar_parse_pharfile function in ext/phar/phar.c.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	99607
CVE	CVE-2017-11147
URL	https://bugs.php.net/bug.php?id=73773

Vulnerability Solution:

•Upgrade to PHP version 5.6.30

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

•Upgrade to PHP version 7.0.15

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

3.2.112. PHP possible overflow inside memnstr (php-possible-overflow-inside-memnstr)

Description:

Buffer overflow in the memnstr function in PHP 4.4.x before 4.4.9 and PHP 5.6 through 5.2.6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via the delimiter argument to the explode function. NOTE: the scope of this issue is limited since most applications would not use an attacker-controlled delimiter, but local attacks against safe_mode are feasible.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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
CERT	TA09-133A
CVE	CVE-2008-3659
DEBIAN	DSA-1647
XF	44405

Vulnerability Solution:

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

3.2.113. TLS/SSL Server Supports DES and IDEA Cipher Suites (ssl-des-ciphers)

Description:

Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) include cipher suites based on the DES (Data Encryption Standard) and IDEA (International Data Encryption Algorithm) algorithms. DES and IDEA algorithms are no longer recommended for general use in TLS, and have been removed from TLS version 1.2.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:443	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_IDEA_CBC_SHATLS 1.1 ciphers: TLS_RSA_WITH_IDEA_CBC_SHA

References:

Source	Reference
URL	http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295
URL	https://wiki.mozilla.org/Security/Server_Side_TLS
URL	https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Rule_-_Only_Support_Strong_Cryptographic_Ciphers
URL	http://support.microsoft.com/kb/245030/
URL	https://tools.ietf.org/html/rfc5469

Vulnerability Solution:

Configure the server to disable support for DES and IDEA cipher suites.
For Microsoft IIS web servers, see Microsoft Knowledgebase article 245030 for instructions on disabling DES and IDEA cipher suites.
The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.
Refer to your server vendor documentation to apply the recommended cipher configuration:
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

3.2.114. 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:
192.168.234.130:443	TLS/SSL certificate signed by unknown, untrusted CA: CN=localhost -- [Path does not chain with any of the trust anchors].
192.168.234.131:5432	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

3.2.115. VMware Player: Arbitrary code execution and denial of service vulnerabilities (VMSA-2007-0006) (CVE-2007-4497) (vmsa-2007-0006-cve-2007-4497-player)

Description:

Unspecified vulnerability in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 55017, Player before 1.0.5 Build 56455 and Player 2 before 2.0.1 Build 55017, ACE before 1.0.3 Build 54075 and ACE 2 before 2.0.1 Build 55017, and Server before 1.0.4 Build 56528 allows users with login access to a guest operating system to cause a denial of service (guest outage and host process crash or hang) via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	25731
CVE	CVE-2007-4497
URL	http://www.vmware.com/security/advisories/VMSA-2007-0006.html

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.5

Upgrade to VMware Player version 1.0.5

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.0 and < 2.0.1

Upgrade to VMware Player version 2.0.1

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.116. VMware Workstation: Arbitrary code execution and denial of service vulnerabilities (VMSA-2007-0006) (CVE-2007-4497) (vmsa-2007-0006-cve-2007-4497-workstation)

Description:

Unspecified vulnerability in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 55017, Player before 1.0.5 Build 56455 and Player 2 before 2.0.1 Build 55017, ACE before 1.0.3 Build 54075 and ACE 2 before 2.0.1 Build 55017, and Server before 1.0.4 Build 56528 allows users with login access to a guest operating system to cause a denial of service (guest outage and host process crash or hang) via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	25731
CVE	CVE-2007-4497
URL	http://www.vmware.com/security/advisories/VMSA-2007-0006.html

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.5

Upgrade to VMware Workstation version 5.5.5

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6 and < 6.0.1

Upgrade to VMware Workstation version 6.0.1

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.2.117. VMware Player: ACE shared folders vulnerability (VMSA-2009-0005) (CVE-2009-0908) (vmsa-2009-0005-cve-2009-0908-player)

Description:

Unspecified vulnerability in the ACE shared folders implementation in the VMware Host Guest File System (HGFS) shared folders feature in VMware ACE 2.5.1 and earlier allows attackers to enable a disabled shared folder.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	34373
CVE	CVE-2009-0908
OVAL	6399
URL	http://www.vmware.com/security/advisories/VMSA-2009-0005.html

Vulnerability Solution:

VMware Player >= 2.5 and < 2.5.2
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.118. VMware Player: Multiple vulnerabilities in mount.vmhgfs (VMSA-2011-0009) (CVE-2011-2145) (vmsa-2011-0009-cve-2011-2145-player)

Description:

mount.vmhgfs in the VMware Host Guest File System (HGFS) in VMware Workstation 7.1.x before 7.1.4, VMware Player 3.1.x before 3.1.4, VMware Fusion 3.1.x before 3.1.3, VMware ESXi 3.5 through 4.1, and VMware ESX 3.0.3 through 4.1, when a Solaris or FreeBSD guest OS is used, allows guest OS users to modify arbitrary guest OS files via unspecified vectors, related to a "procedural error."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Player

References:

Source	Reference
BID	48098
CVE	CVE-2011-2145
DISA_SEVERITY	Category I
DISA_VMSKEY	V0028311
IAVM	2011-A-0075
URL	http://www.vmware.com/security/advisories/VMSA-2011-0009.html
XF	67815

Vulnerability Solution:
VMware Player >= 3.1 and < 3.1.4
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.119. VMware Workstation: Multiple vulnerabilities in mount.vmhgfs (VMSA-2011-0009) (CVE-2011-2145) (vmsa-2011-0009-cve-2011-2145-workstation)

Description:

mount.vmhgfs in the VMware Host Guest File System (HGFS) in VMware Workstation 7.1.x before 7.1.4, VMware Player 3.1.x before 3.1.4, VMware Fusion 3.1.x before 3.1.3, VMware ESXi 3.5 through 4.1, and VMware ESX 3.0.3 through 4.1, when a Solaris or FreeBSD guest OS is used, allows guest OS users to modify arbitrary guest OS files via unspecified vectors, related to a "procedural error."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	48098
CVE	CVE-2011-2145
DISA_SEVERITY	Category I
DISA_VMSKEY	V0028311
IAVM	2011-A-0075
URL	http://www.vmware.com/security/advisories/VMSA-2011-0009.html
XF	67815

Vulnerability Solution:

VMware Workstation >= 7 and < 7.1.4
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.2.120. VMware Player: Guest privilege escalation in VMware Tools (VMSA-2014-0005) (CVE-2014-3793) (vmsa-2014-0005-cve-2014-3793-player)

Description:

VMware Tools in VMware Workstation 10.x before 10.0.2, VMware Player 6.x before 6.0.2, VMware Fusion 6.x before 6.0.3, and VMware ESXi 5.0 through 5.5, when a Windows 8.1 guest OS is used, allows guest OS users to gain guest OS privileges or cause a denial of service (kernel NULL pointer dereference and guest OS crash) via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
CVE	CVE-2014-3793
DISA_SEVERITY	Category I

Source	Reference
DISA_VMSKEY	V0051851
DISA_VMSKEY	V0051855
DISA_VMSKEY	V0051857
IAVM	2014-B-0068
IAVM	2014-B-0069
IAVM	2014-B-0070
URL	http://www.vmware.com/security/advisories/VMSA-2014-0005.html

Vulnerability Solution:

VMware Player >= 6.0 and < 6.0.2
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.121. VMware Workstation: Guest privilege escalation in VMware Tools (VMSA-2014-0005) (CVE-2014-3793) (vmsa-2014-0005-cve-2014-3793-workstation)

Description:

VMware Tools in VMware Workstation 10.x before 10.0.2, VMware Player 6.x before 6.0.2, VMware Fusion 6.x before 6.0.3, and VMware ESXi 5.0 through 5.5, when a Windows 8.1 guest OS is used, allows guest OS users to gain guest OS privileges or cause a denial of service (kernel NULL pointer dereference and guest OS crash) via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
CVE	CVE-2014-3793
DISA_SEVERITY	Category I
DISA_VMSKEY	V0051851
DISA_VMSKEY	V0051855
DISA_VMSKEY	V0051857
IAVM	2014-B-0068
IAVM	2014-B-0069
IAVM	2014-B-0070
URL	http://www.vmware.com/security/advisories/VMSA-2014-0005.html

Vulnerability Solution:

VMware Workstation >= 10 and < 10.0.2
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

3.2.122. VMware Player: Vulnerability (VMSA-2015-0001) (CVE-2014-8370) (vmsa-2015-0001-cve-2014-8370-player)

Description:

VMware Workstation 10.x before 10.0.5, VMware Player 6.x before 6.0.5, VMware Fusion 6.x before 6.0.5, and VMware ESXi 5.0 through 5.5 allow host OS users to gain host OS privileges or cause a denial of service (arbitrary write to a file) by modifying a configuration file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	72338
CVE	CVE-2014-8370
DISA_SEVERITY	Category I
DISA_VMSKEY	V0058513
DISA_VMSKEY	V0058515
DISA_VMSKEY	V0058517
DISA_VMSKEY	V0058535
IAVM	2015-A-0029
IAVM	2015-B-0012
IAVM	2015-B-0013
IAVM	2015-B-0014
URL	http://www.vmware.com/security/advisories/VMSA-2015-0001.html
XF	100933

Vulnerability Solution:

VMware Player >= 6.0 and < 6.0.5
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.123. VMware Workstation: Vulnerability (VMSA-2015-0001) (CVE-2014-8370) (vmsa-2015-0001-cve-2014-8370-workstation)

Description:

VMware Workstation 10.x before 10.0.5, VMware Player 6.x before 6.0.5, VMware Fusion 6.x before 6.0.5, and VMware ESXi 5.0 through 5.5 allow host OS users to gain host OS privileges or cause a denial of service (arbitrary write to a file) by modifying a configuration file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	72338
CVE	CVE-2014-8370
DISA_SEVERITY	Category I
DISA_VMSKEY	V0058513
DISA_VMSKEY	V0058515
DISA_VMSKEY	V0058517
DISA_VMSKEY	V0058535
IAVM	2015-A-0029
IAVM	2015-B-0012
IAVM	2015-B-0013
IAVM	2015-B-0014
URL	http://www.vmware.com/security/advisories/VMSA-2015-0001.html
XF	100933

Vulnerability Solution:

VMware Workstation >= 10 and < 10.0.5
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

3.2.124. VMware Player: Vulnerability (VMSA-2015-0004) (CVE-2015-2336) (vmsa-2015-0004-cve-2015-2336-player)

Description:

TPView.dll in VMware Workstation 10.x before 10.0.6 and 11.x before 11.1.1, VMware Player 6.x before 6.0.6 and 7.x before 7.1.1, and VMware Horizon Client 3.2.x before 3.2.1, 3.3.x, and 5.x local-mode before 5.4.2 on Windows does not properly allocate memory, which allows guest OS users to execute arbitrary code on the host OS via unspecified vectors, a different vulnerability than CVE-2012-0897.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	75095
CVE	CVE-2015-2336
DISA_SEVERITY	Category I
DISA_VMSKEY	V0060965
IAVM	2015-B-0076
URL	http://www.vmware.com/security/advisories/VMSA-2015-0004.html

Vulnerability Solution:

VMware Player >= 6.0 and < 6.0.6
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.125. VMware Workstation: Vulnerability (VMSA-2015-0004) (CVE-2015-2336) (vmsa-2015-0004-cve-2015-2336-workstation)

Description:

TPView.dll in VMware Workstation 10.x before 10.0.6 and 11.x before 11.1.1, VMware Player 6.x before 6.0.6 and 7.x before 7.1.1, and VMware Horizon Client 3.2.x before 3.2.1, 3.3.x, and 5.x local-mode before 5.4.2 on Windows does not properly allocate memory, which allows guest OS users to execute arbitrary code on the host OS via unspecified vectors, a different vulnerability than CVE-2012-0897.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	75095
CVE	CVE-2015-2336
DISA_SEVERITY	Category I

Source	Reference
DISA_VMSKEY	V0060965
IAVM	2015-B-0076
URL	http://www.vmware.com/security/advisories/VMSA-2015-0004.html

Vulnerability Solution:

VMware Workstation >= 10 and < 10.0.5
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

3.2.126. VMware Player: Vulnerability (VMSA-2015-0004) (CVE-2015-2337) (vmsa-2015-0004-cve-2015-2337-player)

Description:

TPInt.dll in VMware Workstation 10.x before 10.0.6 and 11.x before 11.1.1, VMware Player 6.x before 6.0.6 and 7.x before 7.1.1, and VMware Horizon Client 3.2.x before 3.2.1, 3.3.x, and 5.x local-mode before 5.4.2 on Windows does not properly allocate memory, which allows guest OS users to execute arbitrary code on the host OS via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	75095
CVE	CVE-2015-2337
DISA_SEVERITY	Category I
DISA_VMSKEY	V0060965
IAVM	2015-B-0076
URL	http://www.vmware.com/security/advisories/VMSA-2015-0004.html

Vulnerability Solution:

VMware Player >= 6.0 and < 6.0.6
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.127. VMware Workstation: Vulnerability (VMSA-2015-0004) (CVE-2015-2337) (vmsa-2015-0004-cve-2015-2337-workstation)

Description:

TPInt.dll in VMware Workstation 10.x before 10.0.6 and 11.x before 11.1.1, VMware Player 6.x before 6.0.6 and 7.x before 7.1.1, and VMware Horizon Client 3.2.x before 3.2.1, 3.3.x, and 5.x local-mode before 5.4.2 on Windows does not properly allocate memory,

which allows guest OS users to execute arbitrary code on the host OS via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	75095
CVE	CVE-2015-2337
DISA_SEVERITY	Category I
DISA_VMSKEY	V0060965
IAVM	2015-B-0076
URL	http://www.vmware.com/security/advisories/VMSA-2015-0004.html

Vulnerability Solution:
VMware Workstation >= 10 and < 10.0.5
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

3.2.128. VMware Player: Vulnerability (VMSA-2015-0004) (CVE-2015-2338) (vmsa-2015-0004-cve-2015-2338-player)

Description:

TPview.dll in VMware Workstation 10.x before 10.0.6 and 11.x before 11.1.1, VMware Player 6.x before 6.0.6 and 7.x before 7.1.1, and VMware Horizon Client 3.2.x before 3.2.1, 3.3.x, and 5.x local-mode before 5.4.2 on Windows does not properly allocate memory, which allows guest OS users to cause a host OS denial of service via unspecified vectors, a different vulnerability than CVE-2015-2339.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	75092
CVE	CVE-2015-2338
DISA_SEVERITY	Category I
DISA_VMSKEY	V0060965

Source	Reference
IAVM	2015-B-0076
URL	http://www.vmware.com/security/advisories/VMSA-2015-0004.html

Vulnerability Solution:

VMware Player >= 6.0 and < 6.0.6
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.129. VMware Workstation: Vulnerability (VMSA-2015-0004) (CVE-2015-2338) (vmsa-2015-0004-cve-2015-2338-workstation)

Description:

TPview.dll in VMware Workstation 10.x before 10.0.6 and 11.x before 11.1.1, VMware Player 6.x before 6.0.6 and 7.x before 7.1.1, and VMware Horizon Client 3.2.x before 3.2.1, 3.3.x, and 5.x local-mode before 5.4.2 on Windows does not properly allocate memory, which allows guest OS users to cause a host OS denial of service via unspecified vectors, a different vulnerability than CVE-2015-2339.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	75092
CVE	CVE-2015-2338
DISA_SEVERITY	Category I
DISA_VMSKEY	V0060965
IAVM	2015-B-0076
URL	http://www.vmware.com/security/advisories/VMSA-2015-0004.html

Vulnerability Solution:

VMware Workstation >= 10 and < 10.0.5
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

3.2.130. VMware Player: Vulnerability (VMSA-2015-0004) (CVE-2015-2339) (vmsa-2015-0004-cve-2015-2339-player)

Description:

TPview.dll in VMware Workstation 10.x before 10.0.6 and 11.x before 11.1.1, VMware Player 6.x before 6.0.6 and 7.x before 7.1.1, and VMware Horizon Client 3.2.x before 3.2.1, 3.3.x, and 5.x local-mode before 5.4.2 on Windows does not properly allocate memory, which allows guest OS users to cause a host OS denial of service via unspecified vectors, a different vulnerability than CVE-2015-2338.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	75092
CVE	CVE-2015-2339
DISA_SEVERITY	Category I
DISA_VMSKEY	V0060965
IAVM	2015-B-0076
URL	http://www.vmware.com/security/advisories/VMSA-2015-0004.html

Vulnerability Solution:

VMware Player >= 6.0 and < 6.0.6
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.131. VMware Workstation: Vulnerability (VMSA-2015-0004) (CVE-2015-2339) (vmsa-2015-0004-cve-2015-2339-workstation)

Description:

TPview.dll in VMware Workstation 10.x before 10.0.6 and 11.x before 11.1.1, VMware Player 6.x before 6.0.6 and 7.x before 7.1.1, and VMware Horizon Client 3.2.x before 3.2.1, 3.3.x, and 5.x local-mode before 5.4.2 on Windows does not properly allocate memory, which allows guest OS users to cause a host OS denial of service via unspecified vectors, a different vulnerability than CVE-2015-2338.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	75092
CVE	CVE-2015-2339
DISA_SEVERITY	Category I
DISA_VMSKEY	V0060965

Source	Reference
IAVM	2015-B-0076
URL	http://www.vmware.com/security/advisories/VMSA-2015-0004.html

Vulnerability Solution:

VMware Workstation >= 10 and < 10.0.5
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

3.2.132. VMware Player: Vulnerability (VMSA-2015-0004) (CVE-2015-2340) (vmsa-2015-0004-cve-2015-2340-player)

Description:

TPInt.dll in VMware Workstation 10.x before 10.0.6 and 11.x before 11.1.1, VMware Player 6.x before 6.0.6 and 7.x before 7.1.1, and VMware Horizon Client 3.2.x before 3.2.1, 3.3.x, and 5.x local-mode before 5.4.2 on Windows does not properly allocate memory, which allows guest OS users to cause a host OS denial of service via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	75092
CVE	CVE-2015-2340
DISA_SEVERITY	Category I
DISA_VMSKEY	V0060965
IAVM	2015-B-0076
URL	http://www.vmware.com/security/advisories/VMSA-2015-0004.html

Vulnerability Solution:

VMware Player >= 6.0 and < 6.0.6
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.133. VMware Workstation: Vulnerability (VMSA-2015-0004) (CVE-2015-2340) (vmsa-2015-0004-cve-2015-2340-workstation)

Description:

TPInt.dll in VMware Workstation 10.x before 10.0.6 and 11.x before 11.1.1, VMware Player 6.x before 6.0.6 and 7.x before 7.1.1, and VMware Horizon Client 3.2.x before 3.2.1, 3.3.x, and 5.x local-mode before 5.4.2 on Windows does not properly allocate memory, which allows guest OS users to cause a host OS denial of service via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	75092
CVE	CVE-2015-2340
DISA_SEVERITY	Category I
DISA_VMSKEY	V0060965
IAVM	2015-B-0076
URL	http://www.vmware.com/security/advisories/VMSA-2015-0004.html

Vulnerability Solution:

VMware Workstation >= 10 and < 10.0.5
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

3.2.134. VMware Workstation: Workstation heap overflow via authenticated VNC session (VMSA-2017-0021) (CVE-2017-4933) (vmsa-2017-0021-cve-2017-4933-workstation)

Description:

VMware ESXi (6.5 before ESXi650-201710401-BG), Workstation (12.x before 12.5.8), and Fusion (8.x before 8.5.9) contain a vulnerability that could allow an authenticated VNC session to cause a heap overflow via a specific set of VNC packets resulting in heap corruption. Successful exploitation of this issue could result in remote code execution in a virtual machine via the authenticated VNC session. Note: In order for exploitation to be possible in ESXi, VNC must be manually enabled in a virtual machine's .vmx configuration file. In addition, ESXi must be configured to allow VNC traffic through the built-in firewall.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
CVE	CVE-2017-4933
URL	http://www.vmware.com/security/advisories/VMSA-2017-0021.html

Vulnerability Solution:

VMware Workstation >= 12.5 and < 12.5.8
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

3.2.135. VMware Workstation: Workstation stack overflow via authenticated VNC session (VMSA-2017-0021) (CVE-2017-4941) (vmsa-2017-0021-cve-2017-4941-workstation)

Description:

VMware ESXi (6.0 before ESXi600-201711101-SG, 5.5 ESXi550-201709101-SG), Workstation (12.x before 12.5.8), and Fusion (8.x before 8.5.9) contain a vulnerability that could allow an authenticated VNC session to cause a stack overflow via a specific set of VNC packets. Successful exploitation of this issue could result in remote code execution in a virtual machine via the authenticated VNC session. Note: In order for exploitation to be possible in ESXi, VNC must be manually enabled in a virtual machine's .vmx configuration file. In addition, ESXi must be configured to allow VNC traffic through the built-in firewall.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
CVE	CVE-2017-4941
URL	http://www.vmware.com/security/advisories/VMSA-2017-0021.html

Vulnerability Solution:

VMware Workstation >= 12.5 and < 12.5.8
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

3.2.136. Apache HTTPD: mod_proxy_http DoS (CVE-2008-2364) (apache-httpd-cve-2008-2364)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy_http. Review your web server configuration for validation. A flaw was found in the handling of excessive interim responses from an origin server when using mod_proxy_http. A remote attacker could cause a denial of service or high memory usage.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2008-10-09
BID	29653
BID	31681
CVE	CVE-2008-2364
OVAL	11713
OVAL	6084
OVAL	9577
REDHAT	RHSA-2008:0966
REDHAT	RHSA-2008:0967
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	42987

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.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 < 2.2.9

Upgrade to Apache HTTPD version 2.2.9

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.9.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.137. Apache HTTPD: AllowOverride Options handling bypass (CVE-2009-1195) (apache-httpd-cve-2009-1195)

Description:

The affected asset is vulnerable to this vulnerability ONLY if the AllowOverride directive with certin Options are used. Review your web server configuration for validation. A flaw was found in the handling of the "Options" and "AllowOverride" directives. In configurations using the "AllowOverride" directive with certain "Options=" arguments, local users were not restricted from executing commands from a Server-Side-Include script as intended.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2009-11-09-1
BID	35115
CVE	CVE-2009-1195
DEBIAN	DSA-1816
OVAL	11094
OVAL	12377
OVAL	8704
REDHAT	RHSA-2009:1075
REDHAT	RHSA-2009:1156
SUSE	SUSE-SA:2009:050
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	50808

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.

3.2.138. Apache HTTPD: expat DoS (CVE-2009-3560) (apache-httpd-cve-2009-3560)

Description:

The affected asset is vulnerable to this vulnerability ONLY if an attacker is able to get Apache to parse an untrusted XML document. Review your web server configuration for validation. A buffer over-read flaw was found in the bundled expat library. An attacker who is able to get Apache to parse an untrused XML document (for example through mod_dav) may be able to cause a crash. This crash would only be a denial of service if using the worker MPM.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	37203
CVE	CVE-2009-3560
DEBIAN	DSA-1953
DISA_SEVERITY	Category I
DISA_VMSKEY	V0031252
IAVM	2012-A-0020
OVAL	10613
OVAL	12942
OVAL	6883
REDHAT	RHSA-2011:0896
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.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 < 2.2.17

Upgrade to Apache HTTPD version 2.2.17

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.17.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.

3.2.139. Apache HTTPD: expat DoS (CVE-2009-3720) (apache-httpd-cve-2009-3720)

Description:

The affected asset is vulnerable to this vulnerability ONLY if an attacker is able to get Apache to parse an untrusted XML document. Review your web server configuration for validation. A buffer over-read flaw was found in the bundled expat library. An attacker who is able to get Apache to parse an untrused XML document (for example through mod_dav) may be able to cause a crash. This crash would only be a denial of service if using the worker MPM.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2009-3720
DISA_SEVERITY	Category I
DISA_VMSKEY	V0031252
IAVM	2012-A-0020
OVAL	11019
OVAL	12719
OVAL	7112
REDHAT	RHSA-2010:0002
REDHAT	RHSA-2011:0896
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.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 < 2.2.17

Upgrade to Apache HTTPD version 2.2.17

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.17.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.

3.2.140. Apache HTTPD: mod_proxy_ajp DoS (CVE-2010-0408) (apache-httpd-cve-2010-0408)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy_ajp. Review your web server configuration for validation. mod_proxy_ajp would return the wrong status code if it encountered an error, causing a backend server to be put into an error state until the retry timeout expired. A remote attacker could send malicious requests to trigger this issue, resulting in denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2010-11-10-1
BID	38491
CVE	CVE-2010-0408
DEBIAN	DSA-2035
OVAL	8619
OVAL	9935
REDHAT	RHSA-2010:0168
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache HTTPD >= 2.2 and < 2.2.15
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.15.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.

3.2.141. Apache HTTPD: apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-cve-2010-1623)

Description:

The affected asset is vulnerable to this vulnerability ONLY if Apache processes non-SSL requests. Review your web server configuration for validation. A flaw was found in the apr_brigade_split_line() function of the bundled APR-util library, used to process non-SSL requests. A remote attacker could send requests, carefully crafting the timing of individual bytes, which would slowly consume memory, potentially leading to a denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	43673
CVE	CVE-2010-1623
OVAL	12800
REDHAT	RHSA-2010:0950
REDHAT	RHSA-2011:0896
REDHAT	RHSA-2011:0897
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.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 < 2.2.17

Upgrade to Apache HTTPD version 2.2.17

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.17.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.

3.2.142. Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368) (apache-httpd-cve-2011-3368)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy. Review your web server configuration for validation. An exposure was found when using mod_proxy in reverse proxy mode. In certain configurations using RewriteRule with proxy flag, a remote attacker could cause the reverse proxy to connect to an arbitrary server, possibly disclosing sensitive information from internal web servers not directly accessible to attacker. No update of 1.3 will be released. Patches will be published to http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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
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.

3.2.143. Apache HTTPD: scoreboard parent DoS (CVE-2012-0031) (apache-httpd-cve-2012-0031)

Description:

A flaw was found in the handling of the scoreboard. An unprivileged child process could cause the parent process to crash at shutdown rather than terminate cleanly.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	51407
CVE	CVE-2012-0031
DEBIAN	DSA-2405
REDHAT	RHSA-2012:0128
REDHAT	RHSA-2012:0542
REDHAT	RHSA-2012:0543
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.65

Upgrade to Apache HTTPD version 2.0.65

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.2 and < 2.2.22

Upgrade to Apache HTTPD version 2.2.22

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually

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

3.2.144. Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862) (apache-httpd-cve-2013-1862)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_rewrite. Review your web server configuration for validation. mod_rewrite does not filter terminal escape sequences from logs, which could make it easier for attackers to insert those sequences into terminal emulators containing vulnerabilities related to escape sequences.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	59826
BID	64758
CVE	CVE-2013-1862
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061101
IAVM	2015-A-0149
OVAL	18790
OVAL	19534
REDHAT	RHSA-2013:0815
REDHAT	RHSA-2013:1207
REDHAT	RHSA-2013:1208
REDHAT	RHSA-2013:1209
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.65

Upgrade to Apache HTTPD version 2.0.65

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz

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

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

•Apache HTTPD >= 2.2 and < 2.2.25

Upgrade to Apache HTTPD version 2.2.25

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.25.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.

3.2.145. Apache HTTPD: HTTP Trailers processing bypass (CVE-2013-5704) (apache-httpd-cve-2013-5704)

Description:

HTTP trailers could be used to replace HTTP headers late during request processing, potentially undoing or otherwise confusing modules that examined or modified request headers earlier. This fix adds the "MergeTrailers" directive to restore legacy behavior.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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
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.

3.2.146. 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:
192.168.234.131:80	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

Source	Reference
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.

3.2.147. 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:
192.168.234.131:80	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

Source	Reference
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
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.

3.2.148. 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 https://www.apache.org/security/asf-httpoxy-response.txt

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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
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

Source	Reference
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.

3.2.149. 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:
192.168.234.131:80	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
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.

3.2.150. 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 2.2.32 and later. To permit other .htaccess directives while denying the <Limit > directive, see the AllowOverrideList directive. Source code patch is at; http://www.apache.org/dist/httpd/patches/apply_to_2.2.34/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:
192.168.234.131:80	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
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 >= 2.2 and < 2.2.35

Upgrade to Apache HTTPD version 2.2.35

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.35.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 < 2.4.28

Upgrade to Apache HTTPD version 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.

3.2.151. Apache Tomcat default installation/welcome page installed (apache-tomcat-default-install-page)

Description:

The Tomcat default installation or "Welcome" page is installed on this server. This usually indicates a newly installed server which has not yet been configured properly and which may not be known about.

In many cases, Tomcat is installed along with other applications and the user may not be aware that the web server is running. These servers are rarely patched and rarely monitored, providing hackers with a convenient target that is not likely to trip any alarms.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:8180	Running HTTP serviceProduct Tomcat exists -- Apache TomcatHTTP GET request to http://192.168.234.131:8180/ 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.

3.2.152. Anonymous users can obtain the Windows password policy (cifs-nt-0002)

Description:

Anonymous users can obtain the Windows password policy from the system by using CIFS NULL sessions. The password policy contains sensitive information about minimum password length, password lockout threshold, password lockout duration, etc.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Retrieved domain policy for the METASPLOITABLE domain, with SID S-1-5-21-1042354039-2475377354-766472396

References:

Source	Reference
BID	959
CVE	CVE-2000-1200
XF	4015

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.

3.2.153. Samba Connection Flooding Denial of Service Vulnerability (cifs-samba-connection-flooding-dos)

Description:

The smdb daemon (smbd/service.c) in Samba 3.0.1 through 3.0.22 allows remote attackers to cause a denial of service (memory consumption) via a large number of share connection requests.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:139	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian
192.168.234.131:445	Running CIFS serviceProduct Samba exists -- Samba 3.0.20-DebianVulnerable version of product Samba found -- Samba 3.0.20-Debian

References:

Source	Reference
APPLE	APPLE-SA-2006-11-28
BID	18927
CERT	TA06-333A
CERT-VN	313836
CVE	CVE-2006-3403
DEBIAN	DSA-1110
OVAL	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.

3.2.154. 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:
192.168.234.130:3306	Running MySQL service
192.168.234.131:3306	Running MySQL service
192.168.234.131:5432	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

3.2.155. DNS server allows cache snooping (dns-allows-cache-snooping)

Description:

This DNS server is susceptible to DNS cache snooping, whereby an attacker can make non-recursive queries to a DNS server, looking for records potentially already resolved by this DNS server for other clients. Depending on the response, an attacker can use this information to potentially launch other attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Received 1 answers to a non-recursive query for www.rapid7.com
192.168.234.131:53	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.

3.2.156. ISC BIND: BIND 9 Resolver crashes after logging an error in query.c (CVE-2011-4313) (dns-bind-cve-2011-4313)

Description:

query.c in ISC BIND 9.0.x through 9.6.x, 9.4-ESV through 9.4-ESV-R5, 9.6-ESV through 9.6-ESV-R5, 9.7.0 through 9.7.4, 9.8.0 through 9.8.1, and 9.9.0a1 through 9.9.0b1 allows remote attackers to cause a denial of service (assertion failure and named exit) via unknown vectors related to recursive DNS queries, error logging, and the caching of an invalid record by the resolver.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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
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.

3.2.157. CVE-2012-1033: Ghost Domain Names: Revoked Yet Still Resolvable (dns-bind-cve-2012-1033)

Description:

The resolver in ISC BIND 9 through 9.8.1-P1 overwrites cached server names and TTL values in NS records during the processing of a response to an A record query, which allows remote attackers to trigger continued resolvability of revoked domain names via a "ghost domain names" attack.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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.

3.2.158. ISC BIND: Responses with a malformed class attribute can trigger an assertion failure in db.c (CVE-2015-8000) (dns-bind-cve-2015-8000)

Description:

db.c in named in ISC BIND 9.x before 9.9.8-P2 and 9.10.x before 9.10.3-P2 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a malformed class attribute.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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	79349
CVE	CVE-2015-8000
DEBIAN	DSA-3420
REDHAT	RHSA-2015:2655
REDHAT	RHSA-2015:2656
REDHAT	RHSA-2015:2658
REDHAT	RHSA-2016:0078
REDHAT	RHSA-2016:0079
URL	https://kb.isc.org/article/AA-01317/0

Vulnerability Solution:

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

3.2.159. ISC BIND: A problem parsing resource record signatures for DNAME resource records can lead to an assertion failure in resolver.c or db.c (CVE-2016-1286) (dns-bind-cve-2016-1286)

Description:

named in ISC BIND 9.x before 9.9.8-P4 and 9.10.x before 9.10.3-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted signature record for a DNAME record, related to db.c and resolver.c.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2

Affected Nodes:	Additional Information:
192.168.234.131:53	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
CVE	CVE-2016-1286
DEBIAN	DSA-3511
REDHAT	RHSA-2016:0562
REDHAT	RHSA-2016:0601
URL	https://kb.isc.org/article/AA-01353/0

Vulnerability Solution:

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

3.2.160. ISC BIND: A problem handling responses containing a DNAME answer can lead to an assertion failure (CVE-2016-8864) (dns-bind-cve-2016-8864)

Description:

named in ISC BIND 9.x before 9.9.9-P4, 9.10.x before 9.10.4-P4, and 9.11.x before 9.11.0-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a DNAME record in the answer section of a response to a recursive query, related to db.c and resolver.c.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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	94067
CVE	CVE-2016-8864
DEBIAN	DSA-3703
REDHAT	RHSA-2016:2141

Source	Reference
REDHAT	RHSA-2016:2142
REDHAT	RHSA-2016:2615
REDHAT	RHSA-2016:2871
REDHAT	RHSA-2017:1583
URL	https://kb.isc.org/article/AA-01434/0

Vulnerability Solution:

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

3.2.161. ISC BIND: DNS Cache Poisoning Issue ("Kaminsky bug") (CVE-2008-1447) (dns-kaminsky-bug-bind)

Description:

The DNS protocol, as implemented in (1) BIND 8 and 9 before 9.5.0-P1, 9.4.2-P1, and 9.3.5-P1; (2) Microsoft DNS in Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2; and other implementations allow remote attackers to spoof DNS traffic via a birthday attack that uses in-bailiwick referrals to conduct cache poisoning against recursive resolvers, related to insufficient randomness of DNS transaction IDs and source ports, aka "DNS Insufficient Socket Entropy Vulnerability" or "the Kaminsky bug."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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-2008-07-31
APPLE	APPLE-SA-2008-09-09
APPLE	APPLE-SA-2008-09-12
APPLE	APPLE-SA-2008-09-15
BID	30131
CERT	TA08-190A
CERT	TA08-190B
CERT	TA08-260A
CERT-VN	800113

Source	Reference
CVE	CVE-2008-1447
DEBIAN	DSA-1603
DEBIAN	DSA-1604
DEBIAN	DSA-1605
DEBIAN	DSA-1619
DEBIAN	DSA-1623
DISA_SEVERITY	Category I
DISA_VMSKEY	V0016170
IAVM	2008-A-0045
MS	MS08-037
NETBSD	NetBSD-SA2008-009
OVAL	12117
OVAL	5725
OVAL	5761
OVAL	5917
OVAL	9627
REDHAT	RHSA-2008:0533
REDHAT	RHSA-2008:0789
SUSE	SUSE-SA:2008:033
URL	http://www.isc.org/software/bind/advisories/cve-2008-1447
URL	https://kb.isc.org/article/AA-00924/0
XF	43334
XF	43637

Vulnerability Solution:

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

3.2.162. Nameserver Processes Recursive Queries (dns-processes-recursive-queries)

Description:

Allowing nameservers to process recursive queries coming from any system may, in certain situations, help attackers conduct denial of service or cache poisoning attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Nameserver resolved www.google.com to:www.google.com. 300 IN A 64.233.160.103www.google.com. 300 IN A 64.233.160.104www.google.com. 300 IN A 64.233.160.105www.google.com. 300 IN A 64.233.160.106 www.google.com. 300 IN A 64.233.160.147www.google.com. 300 IN A 64.233.160.99
192.168.234.131:53	Nameserver resolved www.google.com to:www.google.com. 300 IN A 64.233.160.103www.google.com. 300 IN A 64.233.160.104www.google.com. 300 IN A 64.233.160.105www.google.com. 300 IN A 64.233.160.106 www.google.com. 300 IN A 64.233.160.147www.google.com. 300 IN A 64.233.160.99

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.

3.2.163. Debian Linux httpd Vulnerability (http-apache-0007)

Description:

The Debian GNU/Linux 2.1 Apache package by default allows anyone to view /usr/doc via the web, remotely. This is because srm.conf is preconfigured with the line:

Alias /doc/ /usr/doc/

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8HTTP GET request to http://192.168.234.131/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

Source	Reference
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>

3.2.164. PHP 5.2.5 cURL safe_mode bypass (http-php-curl-safe-mode-bypass-other)

Description:

curl/interface.c in the cURL library (aka libcurl) in PHP 5.2.4 and 5.2.5 allows context-dependent attackers to bypass safe_mode and open_basedir restrictions and read arbitrary files via a file:// request containing a \x00 sequence, a different vulnerability than CVE-2006-2563.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2008-07-31
APPLE	APPLE-SA-2008-10-09
BID	27413
BID	29009
BID	31681
CVE	CVE-2007-4850
URL	http://article.gmane.org/gmane.comp.security.full-disclosure/58593
URL	http://www.php.net/releases/5_2_6.php
XF	39852
XF	42134

Vulnerability Solution:

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

3.2.165. PHP Multiple Vulnerabilities Fixed in version 5.2.9 (http-php-multiple-vulns-5-2-9)

Description:

The php_zip_make_relative_path function in php_zip.c in PHP 5.2.x before 5.2.9 allows context-dependent attackers to cause a denial of service (crash) via a ZIP file that contains filenames with relative paths, which is not properly handled during extraction.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-09-10-2
CVE	CVE-2009-1271
CVE	CVE-2009-1272
DEBIAN	DSA-1775
DEBIAN	DSA-1789
REDHAT	RHSA-2009:0350
URL	http://www.php.net/ChangeLog-5.php#5.2.9
URL	http://www.php.net/releases/5_2_9.php

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.9.tar.gz

3.2.166. PHP Multiple Vulnerabilities Fixed in version 5.3.2 (http-php-multiple-vulns-5-3-2)

Description:

Improved LCG entropy.

Fixed safe_mode validation inside tempnam() when the directory path does not end with a /.

Fixed a possible open_basedir/safe_mode bypass in the session extension identified by Grzegorz Stachowiak.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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
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

3.2.167. PHP IMAP toolkit crash: rfc822.c legacy routine buffer overflow (http-php-rfc822-write-address-bof)

Description:

php_imap.c in PHP 5.2.5, 5.2.6, 4.x, and other versions, uses obsolete API calls that allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long IMAP request, which triggers an "rfc822.c legacy routine buffer overflow" error message, related to the rfc822_write_address function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	29829
CERT	TA09-133A
CVE	CVE-2008-2829
XF	43357

Vulnerability Solution:

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

3.2.168. PHP Fixed security issues (CVE-2008-2665) (http-php-safemode-bypass3)

Description:

Directory traversal vulnerability in the posix_access function in PHP 5.2.6 and earlier allows remote attackers to bypass safe_mode restrictions via a .. (dot dot) in an http URL, which results in the URL being canonicalized to a local filename after the safe_mode check has successfully run.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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

3.2.169. MySQL 'DATA DIRECTORY' and 'INDEX DIRECTORY' MyISAM Table Privilege Escalation Vulnerability (mysql-datadir-isam-table-privilege-escalation)

Description:

MySQL 4.1.x before 4.1.24, 5.0.x before 5.0.60, 5.1.x before 5.1.24, and 6.0.x before 6.0.5 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 within the MySQL home data directory, which can point to tables that are created in the future.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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-2008-10-09
APPLE	APPLE-SA-2009-09-10-2
BID	29106
BID	31681

Source	Reference
CVE	CVE-2008-2079
DEBIAN	DSA-1608
OVAL	10133
REDHAT	RHSA-2008:0505
REDHAT	RHSA-2008:0510
REDHAT	RHSA-2008:0768
REDHAT	RHSA-2009:1289
URL	http://bugs.mysql.com/32091
URL	http://dev.mysql.com/doc/refman/5.1/en/news-5-1-23.html
URL	http://dev.mysql.com/doc/refman/6.0/en/news-6-0-4.html
XF	42267

Vulnerability Solution:

•Oracle MySQL >= 4.1 and < 4.1.24

Upgrade to Oracle MySQL version 4.1.24

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 >= 5.0 and < 5.0.60

Upgrade to Oracle MySQL version 5.0.60

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 < 5.1.24

Upgrade to Oracle MySQL version 5.1.24

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 >= 6.0 and < 6.0.5

Upgrade to Oracle MySQL version 6.0.5

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

3.2.170. MySQL my_net_skip_rest Packet Length Denial of Service Vulnerability (mysql-my_net_skip_rest-packet-length-dos)

Description:

The my_net_skip_rest function in sql/net_serv.cc in MySQL 5.0 through 5.0.91 and 5.1 before 5.1.47 allows remote attackers to cause a denial of service (CPU and bandwidth consumption) by sending a large number of packets that exceed the maximum length.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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-2010-11-10-1
CVE	CVE-2010-1849
OVAL	7328

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 < 5.1.47

Upgrade to Oracle MySQL version 5.1.47

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

3.2.171. MySQL MyISAM Table Privilege Check Bypass (mysql-myisam-table-privilege-check-bypass)

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:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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-2008-4097
CVE	CVE-2008-4098
DEBIAN	DSA-1662
OVAL	10591
REDHAT	RHSA-2009:1067
REDHAT	RHSA-2010:0110
URL	http://bugs.mysql.com/bug.php?id=32167
URL	http://lists.mysql.com/commits/50036
URL	http://lists.mysql.com/commits/50773
XF	45648
XF	45649

Vulnerability Solution:

•Oracle MySQL >= 4.1 and < 4.1.25

Upgrade to Oracle MySQL version 4.1.25

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 >= 5.0 and < 5.0.77

Upgrade to Oracle MySQL version 5.0.77

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 < 5.1.32

Upgrade to Oracle MySQL version 5.1.32

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 >= 6.0 and < 6.0.10

Upgrade to Oracle MySQL version 6.0.10

Download and apply the upgrade from: http://downloads.mysql.com/archives.php
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for

example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.172. Exported volume is publicly mountable (nfs-mountd-0002)

Description:

An NFS volume is mountable by everyone. Although this is not necessarily a vulnerability itself, this does not exhibit "best practice" from a security standpoint; mounting privileges should be restricted only to hosts that require them.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:42884	/
192.168.234.131:51094	/

References:

None

Vulnerability Solution:

Restrict mounting privileges to only hosts that require them.

3.2.173. Oracle MySQL Vulnerability: CVE-2010-3833 (oracle-mysql-cve-2010-3833)

Description:

MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 does not properly propagate type errors, which allows remote attackers to cause a denial of service (server crash) via crafted arguments to extreme-value functions such as (1) LEAST and (2) GREATEST, related to KILL_BAD_DATA and a "CREATE TABLE ... SELECT."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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-2010-3833
DEBIAN	DSA-2143
REDHAT	RHSA-2010:0825

Source	Reference
REDHAT	RHSA-2011:0164
XF	64845

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.92

Upgrade to Oracle MySQL version 5.0.92

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

•Oracle MySQL >= 5.1 and < 5.1.51

Upgrade to Oracle MySQL version 5.1.51

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

•Oracle MySQL >= 5.5 and < 5.5.6

Upgrade to Oracle MySQL version 5.5.6

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

3.2.174. Oracle MySQL Vulnerability: CVE-2011-2262 (oracle-mysql-cve-2011-2262)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote attackers to affect availability via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2011-2262
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.2.175. Oracle MySQL Vulnerability: CVE-2012-0116 (oracle-mysql-cve-2012-0116)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect confidentiality and integrity via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0116
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

Download and apply the upgrade from: http://downloads.mysql.com/archives.php
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for

example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.2.176. Oracle MySQL Vulnerability: CVE-2012-0118 (oracle-mysql-cve-2012-0118)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect confidentiality and availability via unknown vectors, a different vulnerability than CVE-2012-0113.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0118
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.2.177. Oracle MySQL Vulnerability: CVE-2012-0486 (oracle-mysql-cve-2012-0486)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0491, CVE-2012-0493, and CVE-2012-0495.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
BID	51514
CVE	CVE-2012-0486
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72527

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.2.178. PHP Crash with URI/file..php (php-crash-with-uri-file-php)

Description:

PHP 4.4.x before 4.4.9, and 5.x through 5.2.6, when used as a FastCGI module, allows remote attackers to cause a denial of service (crash) via a request with multiple dots preceding the extension, as demonstrated using foo..php.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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
CERT	TA09-133A
CVE	CVE-2008-3660
DEBIAN	DSA-1647
OVAL	9597
REDHAT	RHSA-2009:0350
XF	44402

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

3.2.179. PHP Vulnerability: CVE-2006-7243 (php-cve-2006-7243)

Description:

PHP before 5.3.4 accepts the \0 character in a pathname, which might allow context-dependent attackers to bypass intended access restrictions by placing a safe file extension after this character, as demonstrated by .php\0.jpg at the end of the argument to the file_exists function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
BID	44951
CVE	CVE-2006-7243
OVAL	12569
REDHAT	RHSA-2013:1307
REDHAT	RHSA-2013:1615
REDHAT	RHSA-2014:0311

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.180. PHP Vulnerability: CVE-2007-4850 (php-cve-2007-4850)

Description:

curl/interface.c in the cURL library (aka libcurl) in PHP 5.2.4 and 5.2.5 allows context-dependent attackers to bypass safe_mode and open_basedir restrictions and read arbitrary files via a file:// request containing a \x00 sequence, a different vulnerability than CVE-2006-2563.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2008-07-31
APPLE	APPLE-SA-2008-10-09
BID	27413
BID	29009
BID	31681

Source	Reference
CVE	CVE-2007-4850
XF	39852
XF	42134

Vulnerability Solution:

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

3.2.181. PHP Vulnerability: CVE-2008-1384 (php-cve-2008-1384)

Description:

Integer overflow in PHP 5.2.5 and earlier allows context-dependent attackers to cause a denial of service and possibly have unspecified other impact via a printf format parameter with a large width specifier, related to the php_sprintf_appendstring function in formatted_print.c and probably other functions for formatted strings (aka *printf functions).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	28392
CVE	CVE-2008-1384
DEBIAN	DSA-1572
XF	41386

Vulnerability Solution:

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

3.2.182. PHP Vulnerability: CVE-2008-2666 (php-cve-2008-2666)

Description:

Multiple directory traversal vulnerabilities in PHP 5.2.6 and earlier allow context-dependent attackers to bypass safe_mode restrictions by creating a subdirectory named http: and then placing ../ (dot dot slash) sequences in an http URL argument to the (1) chdir or (2) ftok function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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

3.2.183. PHP Vulnerability: CVE-2008-3660 (php-cve-2008-3660)

Description:

PHP 4.4.x before 4.4.9, and 5.x through 5.2.6, when used as a FastCGI module, allows remote attackers to cause a denial of service (crash) via a request with multiple dots preceding the extension, as demonstrated using foo..php.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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
CERT	TA09-133A
CVE	CVE-2008-3660
DEBIAN	DSA-1647
OVAL	9597
REDHAT	RHSA-2009:0350
XF	44402

Vulnerability Solution:

•Upgrade to PHP version 4.4.9

Download and apply the upgrade from: http://museum.php.net/php4/php-4.4.9.tar.gz

•Upgrade to PHP version 5.2.7

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

3.2.184. PHP Vulnerability: CVE-2008-4107 (php-cve-2008-4107)

Description:

The (1) rand and (2) mt_rand functions in PHP 5.2.6 do not produce cryptographically strong random numbers, which allows attackers to leverage exposures in products that rely on these functions for security-relevant functionality, as demonstrated by the password-reset functionality in Joomla! 1.5.x and WordPress before 2.6.2, a different vulnerability than CVE-2008-2107, CVE-2008-2108, and CVE-2008-4102.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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

3.2.185. PHP Vulnerability: CVE-2008-5498 (php-cve-2008-5498)

Description:

Array index error in the imageRotate function in PHP 5.2.8 and earlier allows context-dependent attackers to read the contents of arbitrary memory locations via a crafted value of the third argument (aka the bgd_color or clrBack argument) for an indexed image.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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

3.2.186. PHP Vulnerability: CVE-2009-1271 (php-cve-2009-1271)

Description:

The JSON_parser function (ext/json/JSON_parser.c) in PHP 5.2.x before 5.2.9 allows remote attackers to cause a denial of service (segmentation fault) via a malformed string to the json_decode API function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2009-09-10-2
CVE	CVE-2009-1271
DEBIAN	DSA-1775
DEBIAN	DSA-1789
REDHAT	RHSA-2009:0350
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

3.2.187. PHP Vulnerability: CVE-2009-1272 (php-cve-2009-1272)

Description:

The php_zip_make_relative_path function in php_zip.c in PHP 5.2.x before 5.2.9 allows context-dependent attackers to cause a denial of service (crash) via a ZIP file that contains filenames with relative paths, which is not properly handled during extraction.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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

3.2.188. PHP Vulnerability: CVE-2009-3557 (php-cve-2009-3557)

Description:

The tempnam function in ext/standard/file.c in PHP before 5.2.12 and 5.3.x before 5.3.1 allows context-dependent attackers to bypass safe_mode restrictions, and create files in group-writable or world-writable directories, via the dir and prefix arguments.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
CVE	CVE-2009-3557
OVAL	7396
URL	http://www.php.net/ChangeLog-5.php
URL	http://www.php.net/releases/5_3_1.php

Vulnerability Solution:

•Upgrade to PHP version 5.2.12

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

•Upgrade to PHP version 5.3.1

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

3.2.189. PHP Vulnerability: CVE-2010-2484 (php-cve-2010-2484)

Description:

The strrchr function in PHP 5.2 before 5.2.14 allows context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2010-08-24-1
APPLE	APPLE-SA-2010-11-10-1
CVE	CVE-2010-2484

Vulnerability Solution:

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

3.2.190. PHP Vulnerability: CVE-2011-1466 (php-cve-2011-1466)

Description:

Integer overflow in the SdnToJulian function in the Calendar extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a large integer in the first argument to the cal_from_jd function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2011-10-12-3
BID	46967
CVE	CVE-2011-1466
DEBIAN	DSA-2266
REDHAT	RHSA-2011:1423
REDHAT	RHSA-2012:0071

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.6.tar.gz

3.2.191. PHP Vulnerability: CVE-2011-2483 (php-cve-2011-2483)

Description:

crypt_blowfish before 1.1, as used in PHP before 5.3.7 on certain platforms, PostgreSQL before 8.4.9, and other products, does not properly handle 8-bit characters, which makes it easier for context-dependent attackers to determine a cleartext password by leveraging knowledge of a password hash.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2012-02-01-1
BID	49241
CVE	CVE-2011-2483
DEBIAN	DSA-2340
DEBIAN	DSA-2399
REDHAT	RHSA-2011:1377
REDHAT	RHSA-2011:1378
REDHAT	RHSA-2011:1423
SUSE	SUSE-SA:2011:035
XF	69319

Vulnerability Solution:

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

3.2.192. PHP Vulnerability: CVE-2011-4885 (php-cve-2011-4885)

Description:

PHP before 5.3.9 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2012-05-09-1
BID	51193
CERT-VN	903934
CVE	CVE-2011-4885
DEBIAN	DSA-2399
REDHAT	RHSA-2012:0019
REDHAT	RHSA-2012:0071
XF	72021

Vulnerability Solution:

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

3.2.193. PHP Vulnerability: CVE-2012-0789 (php-cve-2012-0789)

Description:

Memory leak in the timezone functionality in PHP before 5.3.9 allows remote attackers to cause a denial of service (memory consumption) by triggering many strtotime function calls, which are not properly handled by the php_date_parse_tzfile cache.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2012-0789

Vulnerability Solution:

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

3.2.194. PHP Vulnerability: CVE-2013-1643 (php-cve-2013-1643)

Description:

The SOAP parser in PHP before 5.3.23 and 5.4.x before 5.4.13 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-1824.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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/

3.2.195. PHP Vulnerability: CVE-2013-6501 (php-cve-2013-6501)

Description:

The default soap.wsdl_cache_dir setting in (1) php.ini-production and (2) php.ini-development in PHP through 5.6.7 specifies the /tmp directory, which makes it easier for local users to conduct WSDL injection attacks by creating a file under /tmp with a predictable filename that is used by the get_sdl function in ext/soap/php_sdl.c.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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/

3.2.196. PHP Vulnerability: CVE-2015-3412 (php-cve-2015-3412)

Description:

PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read arbitrary files via crafted input to an application that calls the stream_resolve_include_path function in ext/standard/streamsfuncs.c, as demonstrated by a filename\0.extension attack that bypasses an intended configuration in which client users may read files with only one specific extension.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	75250
CVE	CVE-2015-3412
REDHAT	RHSA-2015:1135
REDHAT	RHSA-2015:1186

Source	Reference
REDHAT	RHSA-2015:1187
REDHAT	RHSA-2015:1218
URL	https://bugs.php.net/bug.php?id=69353

Vulnerability Solution:

•Upgrade to PHP version 5.4.40

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

•Upgrade to PHP version 5.5.24

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

•Upgrade to PHP version 5.6.8

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

3.2.197. PHP Vulnerability: CVE-2015-4024 (php-cve-2015-4024)

Description:

Algorithmic complexity vulnerability in the multipart_buffer_headers function in main/rfc1867.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote attackers to cause a denial of service (CPU consumption) via crafted form data that triggers an improper order-of-growth outcome.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2015-08-13-2
BID	74903
CVE	CVE-2015-4024
DEBIAN	DSA-3280
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061337
IAVM	2015-A-0199
REDHAT	RHSA-2015:1135
REDHAT	RHSA-2015:1186
REDHAT	RHSA-2015:1187

Source	Reference
REDHAT	RHSA-2015:1218
REDHAT	RHSA-2015:1219

Vulnerability Solution:

•Upgrade to PHP version 5.4.41

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

•Upgrade to PHP version 5.5.25

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

•Upgrade to PHP version 5.6.9

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

3.2.198. PHP Vulnerability: CVE-2015-4148 (php-cve-2015-4148)

Description:

The do_soap_call function in ext/soap/soap.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 does not verify that the uri property is a string, which allows remote attackers to obtain sensitive information by providing crafted serialized data with an int data type, related to a "type confusion" issue.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2015-08-13-2
BID	75103
CVE	CVE-2015-4148
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061337
IAVM	2015-A-0199
REDHAT	RHSA-2015:1053
REDHAT	RHSA-2015:1066
REDHAT	RHSA-2015:1135
REDHAT	RHSA-2015:1218

Vulnerability Solution:

•Upgrade to PHP version 5.4.39

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

•Upgrade to PHP version 5.5.23

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

•Upgrade to PHP version 5.6.7

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

3.2.199. PHP Vulnerability: CVE-2015-6837 (php-cve-2015-6837)

Description:

The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13, when libxml2 before 2.9.2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation during initial error checking, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted XML document, a different vulnerability than CVE-2015-6838.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	76738
CVE	CVE-2015-6837
DEBIAN	DSA-3358
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061365
IAVM	2015-B-0108

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/

3.2.200. PHP Vulnerability: CVE-2015-6838 (php-cve-2015-6838)

Description:

The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13, when libxml2 before 2.9.2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation after the principal argument loop, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted XML document, a different vulnerability than CVE-2015-6837.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	76733
CVE	CVE-2015-6838
DEBIAN	DSA-3358
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061365
IAVM	2015-B-0108

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/

3.2.201. 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:
192.168.234.131:80	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

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/

3.2.202. PHP Vulnerability: CVE-2015-8873 (php-cve-2015-8873)

Description:

Stack consumption vulnerability in Zend/zend_exceptions.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to cause a denial of service (segmentation fault) via recursive method calls.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2015-8873
REDHAT	RHSA-2016:2750

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/

3.2.203. PHP Vulnerability: CVE-2015-8874 (php-cve-2015-8874)

Description:

Stack consumption vulnerability in GD in PHP before 5.6.12 allows remote attackers to cause a denial of service via a crafted imagefilltoborder call.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2015-8874
DEBIAN	DSA-3587
REDHAT	RHSA-2016:2750

Vulnerability Solution:

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

3.2.204. 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:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference

Source	Reference
CVE	CVE-2015-8879
REDHAT	RHSA-2016:2750

Vulnerability Solution:

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

3.2.205. PHP Vulnerability: CVE-2016-10158 (php-cve-2016-10158)

Description:

The exif_convert_any_to_int function in ext/exif/exif.c in PHP before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (application crash) via crafted EXIF data that triggers an attempt to divide the minimum representable negative integer by -1.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	95764
CVE	CVE-2016-10158
DEBIAN	DSA-3783

Vulnerability Solution:

•Upgrade to PHP version 5.6.30

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

•Upgrade to PHP version 7.0.15

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

•Upgrade to PHP version 7.1.1

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

3.2.206. PHP Vulnerability: CVE-2016-10161 (php-cve-2016-10161)

Description:

The object_common1 function in ext/standard/var_unserializer.c in PHP before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (buffer over-read and application crash) via crafted serialized data that is mishandled in a finish_nested_data call.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	95768
CVE	CVE-2016-10161
DEBIAN	DSA-3783

Vulnerability Solution:

•Upgrade to PHP version 5.6.30

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

•Upgrade to PHP version 7.0.15

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

•Upgrade to PHP version 7.1.1

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

3.2.207. PHP Vulnerability: CVE-2016-10397 (php-cve-2016-10397)

Description:

In PHP before 5.6.28 and 7.x before 7.0.13, incorrect handling of various URI components in the URL parser could be used by attackers to bypass hostname-specific URL checks, as demonstrated by evil.example.com:80#@good.example.com/ and evil.example.com:80?@good.example.com/ inputs to the parse_url function (implemented in the php_url_parse_ex function in ext/standard/url.c).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	99552
CVE	CVE-2016-10397

Source	Reference
URL	https://bugs.php.net/bug.php?id=73192

Vulnerability Solution:

•Upgrade to PHP version 5.6.28

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

•Upgrade to PHP version 7.0.13

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

3.2.208. PHP Vulnerability: CVE-2016-10712 (php-cve-2016-10712)

Description:

In PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3, all of the return values of stream_get_meta_data can be controlled if the input can be controlled (e.g., during file uploads). For example, a "$uri = stream_get_meta_data(fopen($file, "r"))['uri']" call mishandles the case where $file is data:text/plain;uri=eviluri, -- in other words, metadata can be set by an attacker.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2016-10712
URL	https://bugs.php.net/bug.php?id=71323

Vulnerability Solution:

•Upgrade to PHP version 5.5.32

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

•Upgrade to PHP version 5.6.18

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

•Upgrade to PHP version 7.0.3

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

3.2.209. PHP Vulnerability: CVE-2016-4070 (php-cve-2016-4070)

Description:

** DISPUTED ** Integer overflow in the php_raw_url_encode function in ext/standard/url.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to cause a denial of service (application crash) via a long string to the rawurlencode function. NOTE: the vendor says "Not sure if this qualifies as security issue (probably not)."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2016-05-16-4
BID	85801
CVE	CVE-2016-4070
DEBIAN	DSA-3560
DISA_SEVERITY	Category I
IAVM	2016-B-0160
REDHAT	RHSA-2016:2750

Vulnerability Solution:

•Upgrade to PHP version 5.5.34

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

•Upgrade to PHP version 5.6.20

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

•Upgrade to PHP version 7.0.5

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

3.2.210. PHP Vulnerability: CVE-2016-5385 (php-cve-2016-5385)

Description:

PHP through 7.0.8 does not attempt to address RFC 3875 section 4.1.18 namespace conflicts and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, as demonstrated by (1) an application that makes a getenv('HTTP_PROXY') call or (2) a CGI configuration of PHP, aka an "httpoxy" issue.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	91821
CERT-VN	797896
CVE	CVE-2016-5385
DEBIAN	DSA-3631
DISA_SEVERITY	Category I
IAVM	2016-B-0160
REDHAT	RHSA-2016:1609
REDHAT	RHSA-2016:1610
REDHAT	RHSA-2016:1611
REDHAT	RHSA-2016:1612
REDHAT	RHSA-2016:1613

Vulnerability Solution:

•Upgrade to PHP version 5.5.38

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

•Upgrade to PHP version 5.6.24

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

•Upgrade to PHP version 7.0.9

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

3.2.211. PHP Vulnerability: CVE-2016-7125 (php-cve-2016-7125)

Description:

ext/session/session.c in PHP before 5.6.25 and 7.x before 7.0.10 skips invalid session names in a way that triggers incorrect parsing, which allows remote attackers to inject arbitrary-type session data by leveraging control of a session name, as demonstrated by object injection.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	92552

Source	Reference
CVE	CVE-2016-7125
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/

3.2.212. PHP Vulnerability: CVE-2016-7128 (php-cve-2016-7128)

Description:

The exif_process_IFD_in_TIFF function in ext/exif/exif.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles the case of a thumbnail offset that exceeds the file size, which allows remote attackers to obtain sensitive information from process memory via a crafted TIFF image.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	92564
CVE	CVE-2016-7128
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/

3.2.213. PHP Vulnerability: CVE-2016-7130 (php-cve-2016-7130)

Description:

The php_wddx_pop_element function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via an invalid base64 binary value, as demonstrated by a wddx_deserialize call that mishandles a binary element in a wddxPacket XML document.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	92764
CVE	CVE-2016-7130
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/

3.2.214. PHP Vulnerability: CVE-2016-7131 (php-cve-2016-7131)

Description:

ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via a malformed wddxPacket XML document that is mishandled in a wddx_deserialize call, as demonstrated by a tag that lacks a < (less than) character.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	92768
CVE	CVE-2016-7131
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/

3.2.215. PHP Vulnerability: CVE-2016-7132 (php-cve-2016-7132)

Description:

ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via an invalid wddxPacket XML document that is mishandled in a wddx_deserialize call, as demonstrated by a stray element inside a boolean element, leading to incorrect pop processing.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	92767
CVE	CVE-2016-7132
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/

3.2.216. PHP Vulnerability: CVE-2016-7418 (php-cve-2016-7418)

Description:

The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service (invalid pointer access and out-of-bounds read) or possibly have unspecified other impact via an incorrect boolean element in a wddxPacket XML document, leading to mishandling in a wddx_deserialize call.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	93011
CVE	CVE-2016-7418

Vulnerability Solution:

•Upgrade to PHP version 5.6.26

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

•Upgrade to PHP version 7.0.11

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

3.2.217. PHP Vulnerability: CVE-2016-7478 (php-cve-2016-7478)

Description:

Zend/zend_exceptions.c in PHP, possibly 5.x before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (infinite loop) via a crafted Exception object in serialized data, a related issue to CVE-2015-8876.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	95150
CVE	CVE-2016-7478
URL	https://bugs.php.net/bug.php?id=73093

Vulnerability Solution:

•Upgrade to PHP version 5.6.28

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

•Upgrade to PHP version 7.0.13

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

3.2.218. PHP Vulnerability: CVE-2016-9934 (php-cve-2016-9934)

Description:

ext/wddx/wddx.c in PHP before 5.6.28 and 7.x before 7.0.13 allows remote attackers to cause a denial of service (NULL pointer dereference) via crafted serialized data in a wddxPacket XML document, as demonstrated by a PDORow string.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	94845
CVE	CVE-2016-9934
URL	http://www.php.net/ChangeLog-5.php
URL	http://www.php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=73331

Vulnerability Solution:

•Upgrade to PHP version 5.6.28

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

•Upgrade to PHP version 7.0.13

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

3.2.219. PHP Vulnerability: CVE-2017-11143 (php-cve-2017-11143)

Description:

In PHP before 5.6.31, an invalid free in the WDDX deserialization of boolean parameters could be used by attackers able to inject XML for deserialization to crash the PHP interpreter, related to an invalid free for an empty boolean element in ext/wddx/wddx.c.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	99553
CVE	CVE-2017-11143
DEBIAN	DSA-4081
URL	https://bugs.php.net/bug.php?id=74145

Vulnerability Solution:

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

3.2.220. PHP Vulnerability: CVE-2017-11144 (php-cve-2017-11144)

Description:

In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, the openssl extension PEM sealing code did not check the return value of the OpenSSL sealing function, which could lead to a crash of the PHP interpreter, related to an interpretation conflict for a negative number in ext/openssl/openssl.c, and an OpenSSL documentation omission.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2017-11144
DEBIAN	DSA-4080
DEBIAN	DSA-4081
URL	https://bugs.php.net/bug.php?id=74651

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/

3.2.221. PHP Vulnerability: CVE-2017-11145 (php-cve-2017-11145)

Description:

In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, an error in the date extension's timelib_meridian parsing code could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: the correct fix is in the e8b7698f5ee757ce2c8bd10a192a491a498f891c commit, not the bd77ac90d3bdf31ce2a5251ad92e9e75 gist.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	99550
CVE	CVE-2017-11145
DEBIAN	DSA-4080
DEBIAN	DSA-4081
URL	https://bugs.php.net/bug.php?id=74819

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/

3.2.222. PHP Vulnerability: CVE-2017-16642 (php-cve-2017-16642)

Description:

In PHP before 5.6.32, 7.x before 7.0.25, and 7.1.x before 7.1.11, an error in the date extension's timelib_meridian handling of 'front of' and 'back of' directives could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: this is a different issue than CVE-2017-11145.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	101745
CVE	CVE-2017-16642
DEBIAN	DSA-4080
DEBIAN	DSA-4081
URL	https://bugs.php.net/bug.php?id=75055

Vulnerability Solution:

•Upgrade to PHP version 5.6.32

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

•Upgrade to PHP version 7.0.25

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

•Upgrade to PHP version 7.1.11

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

3.2.223. PHP Fixed security issue in imagerotate() (php-fixed-security-issue-in-imagerotate)

Description:

Array index error in the imageRotate function in PHP 5.2.8 and earlier allows context-dependent attackers to read the contents of arbitrary memory locations via a crafted value of the third argument (aka the bgd_color or clrBack argument) for an indexed image.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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

Source	Reference
XF	47635

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.9.tar.gz

3.2.224. PHP Fixed security issues (CVE-2008-2666) (php-fixed-security-issues-cve-2008-2666)

Description:

Multiple directory traversal vulnerabilities in PHP 5.2.6 and earlier allow context-dependent attackers to bypass safe_mode restrictions by creating a subdirectory named http: and then placing ../ (dot dot slash) sequences in an http URL argument to the (1) chdir or (2) ftok function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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

3.2.225. PHP NULL pointer dereference when processing invalid XML-RPC requests (php-null-pointer-dereference-when-processing-invalid-xml-rpc-requests)

Description:

The xmlrpc extension in PHP 5.3.1 does not properly handle a missing methodName element in the first argument to the xmlrpc_decode_request function, which allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) and possibly have unspecified other impact via a crafted argument.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2010-08-24-1
APPLE	APPLE-SA-2010-11-10-1
BID	38708
CVE	CVE-2010-0397
REDHAT	RHSA-2010:0919

Vulnerability Solution:

•Upgrade to PHP version 5.2.14

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

•Upgrade to PHP version 5.3.3

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.3.tar.gz

3.2.226. PHP possible interruption array leak in strrchr() (php-possible-interruption-array-leak-in-strrchr)

Description:

The strrchr function in PHP 5.2 before 5.2.14 allows context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2010-08-24-1
APPLE	APPLE-SA-2010-11-10-1
CVE	CVE-2010-2484

Vulnerability Solution:

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

3.2.227. .netrc files exist (unix-netrc-files)

Description:

One or more .netrc files were found on the system. These files may contain unencrypted passwords which may be used to attack other systems.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	/.netrc

References:
None

Vulnerability Solution:
Delete all .netrc files on the system. If these files are absolutely required make sure their permissions are set to 600 or more restrictive.

3.2.228. VMware Player: Updated libpng library to version 1.2.22 to address various security vulnerabilities (VMSA-2008-0005) (CVE-2007-5269) (vmsa-2008-0005-cve-2007-5269-player)

Description:

Certain chunk handlers in libpng before 1.0.29 and 1.2.x before 1.2.21 allow remote attackers to cause a denial of service (crash) via crafted (1) pCAL (png_handle_pCAL), (2) sCAL (png_handle_sCAL), (3) tEXt (png_push_read_tEXt), (4) iTXt (png_handle_iTXt), and (5) ztXT (png_handle_ztXt) chunking in PNG images, which trigger out-of-bounds read operations.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
APPLE	APPLE-SA-2008-03-18
APPLE	APPLE-SA-2008-05-28
BID	25956
BID	28276
CERT	TA08-150A
CVE	CVE-2007-5269
DEBIAN	DSA-1750

Source	Reference
OVAL	10614
REDHAT	RHSA-2007:0992
URL	http://www.vmware.com/security/advisories/VMSA-2008-0005.html

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.6

Upgrade to VMware Player version 1.0.6

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.0 and < 2.0.3

Upgrade to VMware Player version 2.0.3

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.229. VMware Workstation: Updated libpng library to version 1.2.22 to address various security vulnerabilities (VMSA-2008-0005) (CVE-2007-5269) (vmsa-2008-0005-cve-2007-5269-workstation)

Description:

Certain chunk handlers in libpng before 1.0.29 and 1.2.x before 1.2.21 allow remote attackers to cause a denial of service (crash) via crafted (1) pCAL (png_handle_pCAL), (2) sCAL (png_handle_sCAL), (3) tEXt (png_push_read_tEXt), (4) iTXt (png_handle_iTXt), and (5) ztXT (png_handle_ztXt) chunking in PNG images, which trigger out-of-bounds read operations.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
APPLE	APPLE-SA-2008-03-18
APPLE	APPLE-SA-2008-05-28
BID	25956
BID	28276
CERT	TA08-150A
CVE	CVE-2007-5269
DEBIAN	DSA-1750
OVAL	10614
REDHAT	RHSA-2007:0992
URL	http://www.vmware.com/security/advisories/VMSA-2008-0005.html

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.6

Upgrade to VMware Workstation version 5.5.6

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6 and < 6.0.3

Upgrade to VMware Workstation version 6.0.3

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.2.230. VMware Player: Denial of service guest to host vulnerability in a virtual device (VMSA-2009-0005) (CVE-2008-4916) (vmsa-2009-0005-cve-2008-4916-player)

Description:

Unspecified vulnerability in a guest virtual device driver in VMware Workstation before 5.5.9 build 126128, and 6.5.1 and earlier 6.x versions; VMware Player before 1.0.9 build 126128, and 2.5.1 and earlier 2.x versions; VMware ACE before 1.0.8 build 125922, and 2.5.1 and earlier 2.x versions; VMware Server 1.x before 1.0.8 build 126538 and 2.0.x before 2.0.1 build 156745; VMware Fusion before 2.0.1; VMware ESXi 3.5; and VMware ESX 3.0.2, 3.0.3, and 3.5 allows guest OS users to cause a denial of service (host OS crash) via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	34373
CVE	CVE-2008-4916
OVAL	6439
URL	http://www.vmware.com/security/advisories/VMSA-2009-0005.html

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.9

Upgrade to VMware Player version 1.0.9

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.5 and < 2.5.1

Upgrade to VMware Player version 2.5.1

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.231. VMware Workstation: Denial of service guest to host vulnerability in a virtual device (VMSA-2009-0005) (CVE-2008-4916) (vmsa-2009-0005-cve-2008-4916-workstation)

Description:

Unspecified vulnerability in a guest virtual device driver in VMware Workstation before 5.5.9 build 126128, and 6.5.1 and earlier 6.x versions; VMware Player before 1.0.9 build 126128, and 2.5.1 and earlier 2.x versions; VMware ACE before 1.0.8 build 125922, and 2.5.1 and earlier 2.x versions; VMware Server 1.x before 1.0.8 build 126538 and 2.0.x before 2.0.1 build 156745; VMware Fusion before 2.0.1; VMware ESXi 3.5; and VMware ESX 3.0.2, 3.0.3, and 3.5 allows guest OS users to cause a denial of service (host OS crash) via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	34373
CVE	CVE-2008-4916
OVAL	6439
URL	http://www.vmware.com/security/advisories/VMSA-2009-0005.html

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.9

Upgrade to VMware Workstation version 5.5.9

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6.5 and < 6.5.1

Upgrade to VMware Workstation version 6.5.1

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

3.2.232. VMware Player: Host code execution vulnerability from a guest operating system (VMSA-2009-0006) (CVE-2008-4916) (vmsa-2009-0006-cve-2008-4916-player)

Description:

Unspecified vulnerability in a guest virtual device driver in VMware Workstation before 5.5.9 build 126128, and 6.5.1 and earlier 6.x versions; VMware Player before 1.0.9 build 126128, and 2.5.1 and earlier 2.x versions; VMware ACE before 1.0.8 build 125922, and 2.5.1 and earlier 2.x versions; VMware Server 1.x before 1.0.8 build 126538 and 2.0.x before 2.0.1 build 156745; VMware Fusion before 2.0.1; VMware ESXi 3.5; and VMware ESX 3.0.2, 3.0.3, and 3.5 allows guest OS users to cause a denial of service (host OS crash) via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	34373
CVE	CVE-2008-4916
OVAL	6439
URL	http://www.vmware.com/security/advisories/VMSA-2009-0006.html

Vulnerability Solution:

VMware Player >= 2.5 and < 2.5.2
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.233. VMware Workstation: Host code execution vulnerability from a guest operating system (VMSA-2009-0006) (CVE-2008-4916) (vmsa-2009-0006-cve-2008-4916-workstation)

Description:

Unspecified vulnerability in a guest virtual device driver in VMware Workstation before 5.5.9 build 126128, and 6.5.1 and earlier 6.x versions; VMware Player before 1.0.9 build 126128, and 2.5.1 and earlier 2.x versions; VMware ACE before 1.0.8 build 125922, and 2.5.1 and earlier 2.x versions; VMware Server 1.x before 1.0.8 build 126538 and 2.0.x before 2.0.1 build 156745; VMware Fusion before 2.0.1; VMware ESXi 3.5; and VMware ESX 3.0.2, 3.0.3, and 3.5 allows guest OS users to cause a denial of service (host OS crash) via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	34373
CVE	CVE-2008-4916
OVAL	6439
URL	http://www.vmware.com/security/advisories/VMSA-2009-0006.html

Vulnerability Solution:

VMware Workstation >= 6.5 and < 6.5.2
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

3.2.234. VMware Player: Potential information leak via hosted networking stack (VMSA-2010-0007) (CVE-2010-1138) (vmsa-2010-0007-cve-2010-1138-player)

Description:

The virtual networking stack in VMware Workstation 7.0 before 7.0.1 build 227600, VMware Workstation 6.5.x before 6.5.4 build 246459 on Windows, VMware Player 3.0 before 3.0.1 build 227600, VMware Player 2.5.x before 2.5.4 build 246459 on Windows, VMware ACE 2.6 before 2.6.1 build 227600 and 2.5.x before 2.5.4 build 246459, VMware Server 2.x, and VMware Fusion 3.0 before 3.0.1 build 232708 and 2.x before 2.0.7 build 246742 allows remote attackers to obtain sensitive information from memory on the host OS by examining received network packets, related to interaction between the guest OS and the host vmware-vmx process.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	39395
CVE	CVE-2010-1138
DISA_SEVERITY	Category I
DISA_VMSKEY	V0023997
IAVM	2010-A-0066
URL	http://www.vmware.com/security/advisories/VMSA-2010-0007.html

Vulnerability Solution:

•VMware Player >= 2.5 and < 2.5.4

Upgrade to VMware Player version 2.5.4

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 3.0 and < 3.0.1

Upgrade to VMware Player version 3.0.1

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.235. VMware Workstation: Potential information leak via hosted networking stack (VMSA-2010-0007) (CVE-2010-1138) (vmsa-2010-0007-cve-2010-1138-workstation)

Description:

The virtual networking stack in VMware Workstation 7.0 before 7.0.1 build 227600, VMware Workstation 6.5.x before 6.5.4 build 246459 on Windows, VMware Player 3.0 before 3.0.1 build 227600, VMware Player 2.5.x before 2.5.4 build 246459 on Windows, VMware ACE 2.6 before 2.6.1 build 227600 and 2.5.x before 2.5.4 build 246459, VMware Server 2.x, and VMware Fusion 3.0 before 3.0.1 build 232708 and 2.x before 2.0.7 build 246742 allows remote attackers to obtain sensitive information from memory on the host

OS by examining received network packets, related to interaction between the guest OS and the host vmware-vmx process.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	39395
CVE	CVE-2010-1138
DISA_SEVERITY	Category I
DISA_VMSKEY	V0023997
IAVM	2010-A-0066
URL	http://www.vmware.com/security/advisories/VMSA-2010-0007.html

Vulnerability Solution:

•VMware Workstation >= 6.5 and < 6.5.4

Upgrade to VMware Workstation version 6.5.4

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

•VMware Workstation >= 7 and < 7.0.1

Upgrade to VMware Workstation version 7.0.1

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.2.236. VMware Player: Third party libpng updated to version 1.2.44 (VMSA-2010-0014) (CVE-2010-2249) (vmsa-2010-0014-cve-2010-2249-player)

Description:

Memory leak in pngrutil.c in libpng before 1.2.44, and 1.4.x before 1.4.3, allows remote attackers to cause a denial of service (memory consumption and application crash) via a PNG image containing malformed Physical Scale (aka sCAL) chunks.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

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

Source	Reference
APPLE	APPLE-SA-2010-11-22-1
APPLE	APPLE-SA-2011-03-02-1
APPLE	APPLE-SA-2011-03-09-2
BID	41174
CVE	CVE-2010-2249
DEBIAN	DSA-2072
URL	http://www.vmware.com/security/advisories/VMSA-2010-0014.html
XF	59816

Vulnerability Solution:

•VMware Player >= 2.5 and < 2.5.5

Upgrade to VMware Player version 2.5.5

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 3.1 and < 3.1.2

Upgrade to VMware Player version 3.1.2

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.237. VMware Workstation: Third party libpng updated to version 1.2.44 (VMSA-2010-0014) (CVE-2010-2249) (vmsa-2010-0014-cve-2010-2249-workstation)

Description:

Memory leak in pngrutil.c in libpng before 1.2.44, and 1.4.x before 1.4.3, allows remote attackers to cause a denial of service (memory consumption and application crash) via a PNG image containing malformed Physical Scale (aka sCAL) chunks.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
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-2010-2249

Source	Reference
DEBIAN	DSA-2072
URL	http://www.vmware.com/security/advisories/VMSA-2010-0014.html
XF	59816

Vulnerability Solution:

•VMware Workstation >= 6.5 and < 6.5.5

Upgrade to VMware Workstation version 6.5.5

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

•VMware Workstation >= 7 and < 7.1.2

Upgrade to VMware Workstation version 7.1.2

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.2.238. VMware Player: Information Disclosure vulnerability in OpenSSL third party library (VMSA-2014-0004) (CVE-2014-0160) (vmsa-2014-0004-cve-2014-0160-player)

Description:

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	66690
CERT	TA14-098A
CERT-VN	720951
CVE	CVE-2014-0160
DEBIAN	DSA-2896
DISA_SEVERITY	Category I
DISA_VMSKEY	V0033046
IAVM	2012-A-0104
REDHAT	RHSA-2014:0376
REDHAT	RHSA-2014:0377

Source	Reference
REDHAT	RHSA-2014:0378
REDHAT	RHSA-2014:0396
SUSE	SUSE-SA:2014:002
URL	http://www.vmware.com/security/advisories/VMSA-2014-0004.html

Vulnerability Solution:

VMware Player >= 6.0 and < 6.0.2
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.239. VMware Workstation: Information Disclosure vulnerability in OpenSSL third party library (VMSA-2014-0004) (CVE-2014-0160) (vmsa-2014-0004-cve-2014-0160-workstation)

Description:

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	66690
CERT	TA14-098A
CERT-VN	720951
CVE	CVE-2014-0160
DEBIAN	DSA-2896
DISA_SEVERITY	Category I
DISA_VMSKEY	V0033046
IAVM	2012-A-0104
REDHAT	RHSA-2014:0376
REDHAT	RHSA-2014:0377
REDHAT	RHSA-2014:0378
REDHAT	RHSA-2014:0396
SUSE	SUSE-SA:2014:002

Source	Reference
URL	http://www.vmware.com/security/advisories/VMSA-2014-0004.html

Vulnerability Solution:

VMware Workstation >= 10 and < 10.0.2
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

3.2.240. VMware Workstation: Branch Target Injection (VMSA-2018-0002) (CVE-2017-5715) (vmsa-2018-0002-cve-2017-5715-workstation)

Description:

Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	102376
CERT-VN	584653
CVE	CVE-2017-5715
DEBIAN	DSA-4120
REDHAT	RHSA-2018:0292
URL	http://www.vmware.com/security/advisories/VMSA-2018-0002.html

Vulnerability Solution:

VMware Workstation >= 12.5 and < 12.5.8
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

3.2.241. VMware Workstation: Bounds Check bypass (VMSA-2018-0002) (CVE-2017-5753) (vmsa-2018-0002-cve-2017-5753-workstation)

Description:

Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	102371
CERT-VN	584653
CVE	CVE-2017-5753
REDHAT	RHSA-2018:0292
URL	http://www.vmware.com/security/advisories/VMSA-2018-0002.html

Vulnerability Solution:

VMware Workstation >= 12.5 and < 12.5.8
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

3.2.242. VMware Workstation: Vulnerability (VMSA-2018-0004) (CVE-2017-5715) (vmsa-2018-0004-cve-2017-5715-workstation)

Description:

Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	102376
CERT-VN	584653
CVE	CVE-2017-5715
DEBIAN	DSA-4120
REDHAT	RHSA-2018:0292

Source	Reference
URL	http://www.vmware.com/security/advisories/VMSA-2018-0004.html

Vulnerability Solution:

•VMware Workstation >= 12.5 and < 12.5.9

Upgrade to VMware Workstation version 12.5.9

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

•VMware Workstation >= 14 and < 14.1.1

Upgrade to VMware Workstation version 14.1.1

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/14_0

3.2.243. Apache HTTPD: mod_proxy_balancer CSRF (CVE-2007-6420) (apache-httpd-cve-2007-6420)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy_balancer. Review your web server configuration for validation. The mod_proxy_balancer provided an administrative interface that could be vulnerable to cross-site request forgery (CSRF) attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2008-10-09
BID	27236
BID	31681
CVE	CVE-2007-6420
OVAL	8371
REDHAT	RHSA-2008:0966
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache HTTPD >= 2.2 and < 2.2.9

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.9.tar.gz

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

operating system.

3.2.244. Apache HTTPD: mod_proxy_ftp globbing XSS (CVE-2008-2939) (apache-httpd-cve-2008-2939)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy_ftp. Review your web server configuration for validation. A flaw was found in the handling of wildcards in the path of a FTP URL with mod_proxy_ftp. If mod_proxy_ftp is enabled to support FTP-over-HTTP, requests containing globbing characters could lead to cross-site scripting (XSS) attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	30560
CERT	TA09-133A
CERT-VN	663763
CVE	CVE-2008-2939
OVAL	11316
OVAL	7716
REDHAT	RHSA-2008:0966
REDHAT	RHSA-2008:0967
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	44223

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.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 < 2.2.10

Upgrade to Apache HTTPD version 2.2.10

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.10.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.

3.2.245. Apache HTTPD: APR-util heap underwrite (CVE-2009-0023) (apache-httpd-cve-2009-0023)

Description:

The affected asset is vulnerable to this vulnerability ONLY if an attacker can provide a specially crafted search keyword to a function that handles compiled forms of search patterns. Review your web server configuration for validation. A heap-based underwrite flaw was found in the way the bundled copy of the APR-util library created compiled forms of particular search patterns. An attacker could formulate a specially-crafted search keyword, that would overwrite arbitrary heap memory locations when processed by the pattern preparation engine.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2009-11-09-1
BID	35221
CVE	CVE-2009-0023
DEBIAN	DSA-1812
OVAL	10968
OVAL	12321
REDHAT	RHSA-2009:1107
REDHAT	RHSA-2009:1108
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	50964

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.

3.2.246. Apache HTTPD: Subrequest handling of request headers (mod_headers) (CVE-2010-0434) (apache-httpd-cve-2010-0434)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_headers. Review your web server configuration for validation. A flaw in the core subrequest process code was fixed, to always provide a shallow copy of the headers_in array to the subrequest, instead of a pointer to the parent request's array as it had for requests without request bodies. This meant all modules such as mod_headers which may manipulate the input headers for a subrequest would poison the parent request in two ways, one by modifying the parent request, which might not be intended, and second by leaving pointers to modified header fields in memory allocated to the subrequest scope, which could be freed before the main request processing was finished, resulting in a segfault or in revealing data from another request on threaded servers, such as the worker or winnt MPMs.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2010-11-10-1
BID	38494
CVE	CVE-2010-0434
DEBIAN	DSA-2035
OVAL	10358
OVAL	8695
REDHAT	RHSA-2010:0168
REDHAT	RHSA-2010:0175
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	56625

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.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 < 2.2.15

Upgrade to Apache HTTPD version 2.2.15

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.15.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.

3.2.247. Apache HTTPD: apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpd-cve-2011-0419)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_autoindex. Review your web server configuration for validation. A flaw was found in the apr_fnmatch() function of the bundled APR library. Where mod_autoindex is enabled, and a directory indexed by mod_autoindex contained files with sufficiently long names, a remote attacker could send a carefully crafted request which would cause excessive CPU usage. This could be used in a denial of service attack. Workaround: Setting the 'IgnoreClient' option to the 'IndexOptions' directive disables processing of the client-supplied request query arguments, preventing this attack. Resolution: Update APR to release 0.9.20 (to be bundled with httpd 2.0.65)

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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
CVE	CVE-2011-0419
DEBIAN	DSA-2237
OVAL	14638
OVAL	14804
REDHAT	RHSA-2011:0507
REDHAT	RHSA-2011:0896
REDHAT	RHSA-2011:0897
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.65

Upgrade to Apache HTTPD version 2.0.65

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.2 and < 2.2.19

Upgrade to Apache HTTPD version 2.2.19

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.19.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.

3.2.248. Apache HTTPD: mod_setenvif .htaccess privilege escalation (CVE-2011-3607) (apache-httpd-cve-2011-3607)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_setenvif. Review your web server configuration for validation. An integer overflow flaw was found which, when the mod_setenvif module is enabled, could allow local users to gain privileges via a .htaccess file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	50494
CVE	CVE-2011-3607
DEBIAN	DSA-2405
REDHAT	RHSA-2012:0128
REDHAT	RHSA-2012:0542
REDHAT	RHSA-2012:0543
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Source	Reference
XF	71093

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.65

Upgrade to Apache HTTPD version 2.0.65

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.2 and < 2.2.22

Upgrade to Apache HTTPD version 2.2.22

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.249. Apache HTTPD: error responses can expose cookies (CVE-2012-0053) (apache-httpd-cve-2012-0053)

Description:

A flaw was found in the default error response for status code 400. This flaw could be used by an attacker to expose "httpOnly" cookies when no custom ErrorDocument is specified.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

192.168.234.131:80	Running HTTP serviceHTTP GET request to http://192.168.234.131/
	HTTP response code was an expected 400
	5: <h1>Bad Request</h1>
	6: <p>Your browser sent a request that this server could not understan...
	7: Request header field is missing ':' separator.
	
	8: <pre>
	9:
	R7TESTR7TESTR7TESTR7TESTR7TESTR7TESTR7TESTR7TESTR7TESTR7TESTR7TESTR7TE...

References:

Source	Reference

Source	Reference
APPLE	APPLE-SA-2012-09-19-2
BID	51706
CVE	CVE-2012-0053
DEBIAN	DSA-2405
REDHAT	RHSA-2012:0128
REDHAT	RHSA-2012:0542
REDHAT	RHSA-2012:0543
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.65

Upgrade to Apache HTTPD version 2.0.65

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.2 and < 2.2.22

Upgrade to Apache HTTPD version 2.2.22

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.250. Apache HTTPD: XSS due to unescaped hostnames (CVE-2012-3499) (apache-httpd-cve-2012-3499)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_imagemap, mod_info, mod_ldap, mod_proxy_ftp, mod_status. Review your web server configuration for validation. Various XSS flaws due to unescaped hostnames and URIs HTML output in mod_info, mod_status, mod_imagemap, mod_ldap, and mod_proxy_ftp.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
BID	58165
BID	64758
CVE	CVE-2012-3499
DEBIAN	DSA-2637
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061101
IAVM	2015-A-0149
OVAL	19312
REDHAT	RHSA-2013:0815
REDHAT	RHSA-2013:1207
REDHAT	RHSA-2013:1208
REDHAT	RHSA-2013:1209
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 < 2.2.24

Upgrade to Apache HTTPD version 2.2.24

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.24.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 < 2.4.4

Upgrade to Apache HTTPD version 2.4.4

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.4.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.

3.2.251. Apache HTTPD: XSS in mod_proxy_balancer (CVE-2012-4558) (apache-httpd-cve-2012-4558)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy_balancer. Review your web server configuration for validation. A XSS flaw affected the mod_proxy_balancer manager interface.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
BID	58165
BID	64758
CVE	CVE-2012-4558
DEBIAN	DSA-2637
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061101
IAVM	2015-A-0149
OVAL	18977
REDHAT	RHSA-2013:0815
REDHAT	RHSA-2013:1207
REDHAT	RHSA-2013:1208
REDHAT	RHSA-2013:1209
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 < 2.2.24

Upgrade to Apache HTTPD version 2.2.24

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.24.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 < 2.4.4

Upgrade to Apache HTTPD version 2.4.4

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.4.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.

3.2.252. Apache HTTPD: mod_deflate denial of service (CVE-2014-0118) (apache-httpd-cve-2014-0118)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_deflate. Review your web server configuration for validation. A resource consumption flaw was found in mod_deflate. If request body decompression was configured (using the "DEFLATE" input filter), a remote attacker could cause the server to consume significant memory and/or CPU resources. The use of request body decompression is not a common configuration.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
BID	68745
CVE	CVE-2014-0118
DEBIAN	DSA-2989
DISA_SEVERITY	Category I
DISA_VMSKEY	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.

3.2.253. Apache HTTPD: Out of bound write in mod_authnz_ldap when using too small Accept-Language values (CVE-2017-15710) (apache-httpd-cve-2017-15710)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_authnz_ldap. Review your web server configuration for validation. mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.29 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.29
192.168.234.130:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPD 2.4.29 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.29

References:

Source	Reference
BID	103512
CVE	CVE-2017-15710
DEBIAN	DSA-4164
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.30

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.30.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.

3.2.254. Apache HTTPD: <FilesMatch> bypass with a trailing newline in the file name (CVE-2017-15715) (apache-httpd-cve-2017-15715)

Description:

The expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.29 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.29
192.168.234.130:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPD 2.4.29 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.29

References:

Source	Reference
BID	103525
CVE	CVE-2017-15715
DEBIAN	DSA-4164
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.30
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.30.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.

3.2.255. Apache HTTPD: Tampering of mod_session data for CGI applications (CVE-2018-1283) (apache-httpd-cve-2018-1283)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_session. Review your web server configuration for validation. When mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications. The severity is set to Moderate because "SessionEnv on" is not a default nor common configuration, it should be considered more severe when this is the case though, because of the possible remote exploitation.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.29 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.29
192.168.234.130:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPD 2.4.29 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.29

References:

Source	Reference
BID	103520
CVE	CVE-2018-1283
DEBIAN	DSA-4164
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.30
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.30.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.

3.2.256. Apache HTTPD: Possible out of bound access after failure in reading the HTTP request (CVE-2018-1301) (apache-httpd-cve-2018-1301)

Description:

A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.29 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.29
192.168.234.130:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPD 2.4.29 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.29

References:

Source	Reference
BID	103515

Source	Reference
CVE	CVE-2018-1301
DEBIAN	DSA-4164
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.30
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.30.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.

3.2.257. Apache HTTPD: Possible write of after free on HTTP/2 stream shutdown (CVE-2018-1302) (apache-httpd-cve-2018-1302)

Description:

When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerabilty hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.29 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.29
192.168.234.130:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPD 2.4.29 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.29

References:

Source	Reference
BID	103528
CVE	CVE-2018-1302
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.30
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.30.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.

3.2.258. Apache HTTPD: Possible out of bound read in mod_cache_socache (CVE-2018-1303) (apache-httpd-cve-2018-1303)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_cache_socache. Review your web server configuration for validation. A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.29 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.29
192.168.234.130:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPD 2.4.29 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.29

References:

Source	Reference
BID	103522
CVE	CVE-2018-1303
DEBIAN	DSA-4164
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.30
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.30.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.

3.2.259. Apache HTTPD: Weak Digest auth nonce generation in mod_auth_digest (CVE-2018-1312) (apache-httpd-cve-2018-1312)

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. When generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.234.130:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.29 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.29
192.168.234.130:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPD 2.4.29 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.29

References:

Source	Reference
BID	103524
CVE	CVE-2018-1312
DEBIAN	DSA-4164
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.30
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.30.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.

3.2.260. 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:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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	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.

3.2.261. 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:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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.

3.2.262. ISC BIND: An error parsing input received by the rndc control channel can cause an assertion failure in sexpr.c or alist.c (CVE-2016-1285) (dns-bind-cve-2016-1285)

Description:

named in ISC BIND 9.x before 9.9.8-P4 and 9.10.x before 9.10.3-P4 does not properly handle DNAME records when parsing fetch reply messages, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed packet to the rndc (aka control channel) interface, related to alist.c and sexpr.c.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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
CVE	CVE-2016-1285
DEBIAN	DSA-3511
REDHAT	RHSA-2016:0562
REDHAT	RHSA-2016:0601
URL	https://kb.isc.org/article/AA-01352/0

Vulnerability Solution:

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

3.2.263. 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:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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.

3.2.264. ISC BIND: Improper fetch cleanup sequencing in the resolver can cause named to crash (CVE-2017-3145) (dns-bind-cve-2017-3145)

Description:

BIND was improperly sequencing cleanup operations on upstream recursion fetch contexts, leading in some cases to a use-after-free error that can trigger an assertion failure and crash in named.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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
CVE	CVE-2017-3145
URL	https://kb.isc.org/article/AA-01542/0

Vulnerability Solution:

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

3.2.265. ISC BIND: BIND Dynamic Update DoS (CVE-2009-0696) (dns-bind-remote-dynamic-update-message-dos)

Description:

The dns_db_findrdataset function in db.c in named in ISC BIND 9.4 before 9.4.3-P3, 9.5 before 9.5.1-P3, and 9.6 before 9.6.1-P1, when configured as a master server, allows remote attackers to cause a denial of service (assertion failure and daemon exit) via an ANY record in the prerequisite section of a crafted dynamic update message, as exploited in the wild in July 2009.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2

Affected Nodes:	Additional Information:
192.168.234.131:53	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
CERT-VN	725188
CVE	CVE-2009-0696
NETBSD	NetBSD-SA2009-013
OVAL	10414
OVAL	12245
OVAL	7806
URL	https://kb.isc.org/article/AA-00926/0
URL	https://kb.isc.org/article/AA-00926/187/CVE-2009-0696%3A-BIND-Dynamic-Update-DoS.html

Vulnerability Solution:

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

3.2.266. Default CGI Script printenv is Executable (http-apache-0011)

Description:

The web server makes a test script available that reveals details of the web server's configuration to anyone who can connect to the machine.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.29HTTP GET request to http://192.168.234.130/cgi-bin/printenv HTTP response code was 404 but expected 200HTTP response code was 404 but expected 200HTTP response code was 404 but expected 200 HTTP GET request to http://192.168.234.130/cgi-bin/printenv.pl HTTP response code was an expected 200 1: COMSPEC="C:\Windows\system32\cmd.exe" 2: CONTEXT_DOCUMENT_ROOT="C:/xampp/cgi-bin/" 3: CONTEXT_PREFIX="/cgi-bin/" 4: DOCUMENT_ROOT="C:/xampp/htdocs"
192.168.234.130:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPD 2.4.29HTTP

Affected Nodes:	Additional Information:
	GET request to https://192.168.234.130/cgi-bin/printenv HTTP response code was 404 but expected 200HTTP response code was 404 but expected 200HTTP response code was 404 but expected 200 HTTP GET request to https://192.168.234.130/cgi-bin/printenv.pl HTTP response code was an expected 200 1: COMSPEC="C:\Windows\system32\cmd.exe" 2: CONTEXT_DOCUMENT_ROOT="C:/xampp/cgi-bin/" 3: CONTEXT_PREFIX="/cgi-bin/" 4: DOCUMENT_ROOT="C:/xampp/htdocs"

References:

None

Vulnerability Solution:

Look for the file "printenv" in your Apache installation tree, usually in a directory called "cgi-bin", either move this file or delete it.

3.2.267. OpenSSL rsaz_1024_mul_avx2 overflow bug on x86_64 (CVE-2017-3738) (http-openssl-cve-2017-3738)

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:80	Running HTTP serviceVulnerable version of component OpenSSL found -- OpenSSL 1.1.0g
192.168.234.130:443	Running HTTPS serviceVulnerable version of component OpenSSL found -- OpenSSL 1.1.0g

References:

Source	Reference
BID	102118

Source	Reference
CVE	CVE-2017-3738
DEBIAN	DSA-4065
DEBIAN	DSA-4157
REDHAT	RHSA-2018:0998
URL	https://www.openssl.org/news/secadv/20171207.txt

Vulnerability Solution:

•Upgrade to OpenSSL version 1.0.2n

Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.2n.tar.gz
Upgrade to version 1.0.2n of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

•Upgrade to OpenSSL version 1.1.0h

Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.1.0h.tar.gz
Upgrade to version 1.1.0h of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.268. OpenSSL Incorrect CRYPTO_memcmp on HP-UX PA-RISC (CVE-2018-0733) (http-openssl-cve-2018-0733)

Description:

Because of an implementation bug the PA-RISC CRYPTO_memcmp function is effectively reduced to only comparing the least significant bit of each byte. This allows an attacker to forge messages that would be considered as authenticated in an amount of tries lower than that guaranteed by the security claims of the scheme. The module can only be compiled by the HP-UX assembler, so that only HP-UX PA-RISC targets are affected. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:80	Running HTTP serviceVulnerable version of component OpenSSL found -- OpenSSL 1.1.0g
192.168.234.130:443	Running HTTPS serviceVulnerable version of component OpenSSL found -- OpenSSL 1.1.0g

References:

Source	Reference

Source	Reference
BID	103517
CVE	CVE-2018-0733
URL	https://www.openssl.org/news/secadv/20180327.txt

Vulnerability Solution:

Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.1.0h.tar.gz
Upgrade to version 1.1.0h of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.269. OpenSSL Constructed ASN.1 types with a recursive definition could exceed the stack (CVE-2018-0739) (http-openssl-cve-2018-0739)

Description:

Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:80	Running HTTP serviceVulnerable version of component OpenSSL found -- OpenSSL 1.1.0g
192.168.234.130:443	Running HTTPS serviceVulnerable version of component OpenSSL found -- OpenSSL 1.1.0g

References:

Source	Reference
BID	103518
CVE	CVE-2018-0739
DEBIAN	DSA-4157
DEBIAN	DSA-4158
URL	https://www.openssl.org/news/secadv/20180327.txt

Vulnerability Solution:

•Upgrade to OpenSSL version 1.0.2o

Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.2o.tar.gz
Upgrade to version 1.0.2o of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most

recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

•Upgrade to OpenSSL version 1.1.0h

Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.1.0h.tar.gz
Upgrade to version 1.1.0h of OpenSSL. The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.270. PHP Multiple Vulnerabilities Fixed in version 5.2.10 (http-php-multiple-vulns-5-2-10)

Description:

The exif_read_data function in the Exif module in PHP before 5.2.10 allows remote attackers to cause a denial of service (crash) via a malformed JPEG image with invalid offset fields, a different issue than CVE-2005-3353.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	35440
CVE	CVE-2009-2687
DEBIAN	DSA-1940
OVAL	10695
OVAL	6655
URL	http://www.php.net/ChangeLog-5.php#5.2.10
URL	http://www.php.net/releases/5_2_10.php
XF	51253

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.10.tar.gz

3.2.271. MySQL Bug #29908: ALTER VIEW Privilege Escalation Vulnerability (mysql-bug-29908-alter-view-priv-esc)

Description:

A flaw in the ALTER VIEW routine of MySQL allows for the opportunity of an authenticated user to elevate their privileges in certain contexts.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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.

3.2.272. MySQL Bug #44798: Stored Procedures Server Crash (mysql-bug-44798-stored-procedures-server-crash)

Description:

Versions of MySQL server 5.0 before 5.0.84 and 5.1 before 5.1.36 suffer from a privilege interpretation flaw that causes a server crash. A user created with the privileges to create stored procedures but not execute them will trigger this issue.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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.

3.2.273. MySQL Empty Bit-String Literal Denial of Service (mysql-empty-bit-string-dos)

Description:

MySQL 5.0 before 5.0.66, 5.1 before 5.1.26, and 6.0 before 6.0.6 does not properly handle a b'' (b single-quote single-quote) token, aka an empty bit-string literal, which allows remote attackers to cause a denial of service (daemon crash) by using this token in a SQL statement.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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-2008-3963
DEBIAN	DSA-1783
OVAL	10521
REDHAT	RHSA-2009:1067
REDHAT	RHSA-2009:1289
URL	http://bugs.mysql.com/bug.php?id=35658
XF	45042

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.66

Upgrade to Oracle MySQL version 5.0.66

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 < 5.1.26

Upgrade to Oracle MySQL version 5.1.26

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 >= 6.0 and < 6.0.6

Upgrade to Oracle MySQL version 6.0.6

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.

3.2.274. MySQL InnoDB Denial of Service (mysql-innodb-dos)

Description:

The convert_search_mode_to_innobase function in ha_innodb.cc in the InnoDB engine in MySQL 5.1.23-BK and earlier allows remote authenticated users to cause a denial of service (database crash) via a certain CONTAINS operation on an indexed column, which triggers an assertion error.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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	26353
CVE	CVE-2007-5925
DEBIAN	DSA-1413
OVAL	11390
REDHAT	RHSA-2007:1155

Source	Reference
REDHAT	RHSA-2007:1157
URL	http://bugs.mysql.com/bug.php?id=32125
XF	38284

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.24

Upgrade to Oracle MySQL version 5.0.24

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.

•Oracle MySQL >= 6.0 and < 6.0.4

Upgrade to Oracle MySQL version 6.0.4

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.

3.2.275. Oracle MySQL Vulnerability: CVE-2009-4019 (oracle-mysql-cve-2009-4019)

Description:

mysqld in MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41 does not (1) properly handle errors during execution of certain SELECT statements with subqueries, and does not (2) preserve certain null_value flags during execution of statements that use the GeomFromWKB function, which allows remote authenticated users to cause a denial of service (daemon crash) via a crafted statement.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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-2010-03-29-1

Source	Reference
CVE	CVE-2009-4019
DEBIAN	DSA-1997
OVAL	11349
OVAL	8500
REDHAT	RHSA-2010:0109

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.

3.2.276. Oracle MySQL Vulnerability: CVE-2010-3677 (oracle-mysql-cve-2010-3677)

Description:

Oracle MySQL 5.1 before 5.1.49 and 5.0 before 5.0.92 allows remote authenticated users to cause a denial of service (mysqld daemon crash) via a join query that uses a table with a unique SET column.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
APPLE	APPLE-SA-2011-06-23-1
BID	42646
CVE	CVE-2010-3677
DEBIAN	DSA-2143
REDHAT	RHSA-2010:0825

Source	Reference
REDHAT	RHSA-2011:0164
XF	64688

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.92

Upgrade to Oracle MySQL version 5.0.92

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

•Oracle MySQL >= 5.1 and < 5.1.49

Upgrade to Oracle MySQL version 5.1.49

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

3.2.277. Oracle MySQL Vulnerability: CVE-2010-3682 (oracle-mysql-cve-2010-3682)

Description:

Oracle MySQL 5.1 before 5.1.49 and 5.0 before 5.0.92 allows remote authenticated users to cause a denial of service (mysqld daemon crash) by using EXPLAIN with crafted "SELECT ... UNION ... ORDER BY (SELECT ... WHERE ...)" statements, which triggers a NULL pointer dereference in the Item_singlerow_subselect::store function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
APPLE	APPLE-SA-2011-06-23-1
BID	42599
CVE	CVE-2010-3682
DEBIAN	DSA-2143
REDHAT	RHSA-2010:0825
REDHAT	RHSA-2011:0164
XF	64684

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.92

Upgrade to Oracle MySQL version 5.0.92

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

•Oracle MySQL >= 5.1 and < 5.1.49

Upgrade to Oracle MySQL version 5.1.49

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

3.2.278. Oracle MySQL Vulnerability: CVE-2010-3834 (oracle-mysql-cve-2010-3834)

Description:

Unspecified vulnerability in MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (server crash) via vectors related to "materializing a derived table that required a temporary table for grouping" and "user variable assignments."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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.

3.2.279. Oracle MySQL Vulnerability: CVE-2010-3836 (oracle-mysql-cve-2010-3836)

Description:

MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (assertion failure and server crash) via vectors related to view preparation, pre-evaluation of LIKE predicates, and IN Optimizers.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
APPLE	APPLE-SA-2011-06-23-1
BID	43676
CVE	CVE-2010-3836
DEBIAN	DSA-2143
REDHAT	RHSA-2010:0825
REDHAT	RHSA-2011:0164
XF	64842

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.92

Upgrade to Oracle MySQL version 5.0.92

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

•Oracle MySQL >= 5.1 and < 5.1.51

Upgrade to Oracle MySQL version 5.1.51

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

•Oracle MySQL >= 5.5 and < 5.5.6

Upgrade to Oracle MySQL version 5.5.6

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

3.2.280. Oracle MySQL Vulnerability: CVE-2010-3837 (oracle-mysql-cve-2010-3837)

Description:

MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (server crash) via a prepared statement that uses GROUP_CONCAT with the WITH ROLLUP modifier, probably triggering a use-after-free error when a copied object is modified in a way that also affects the original object.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
APPLE	APPLE-SA-2011-06-23-1
BID	43676
CVE	CVE-2010-3837
DEBIAN	DSA-2143
REDHAT	RHSA-2010:0825
REDHAT	RHSA-2011:0164
XF	64841

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.92

Upgrade to Oracle MySQL version 5.0.92

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

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

•Oracle MySQL >= 5.1 and < 5.1.51

Upgrade to Oracle MySQL version 5.1.51

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

•Oracle MySQL >= 5.5 and < 5.5.6

Upgrade to Oracle MySQL version 5.5.6

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

3.2.281. Oracle MySQL Vulnerability: CVE-2010-3838 (oracle-mysql-cve-2010-3838)

Description:

MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (server crash) via a query that uses the (1) GREATEST or (2) LEAST function with a mixed list of numeric and LONGBLOB arguments, which is not properly handled when the function's result is "processed using an intermediate temporary table."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
APPLE	APPLE-SA-2011-06-23-1
BID	43676
CVE	CVE-2010-3838
DEBIAN	DSA-2143
REDHAT	RHSA-2010:0825
REDHAT	RHSA-2011:0164
XF	64840

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.92

Upgrade to Oracle MySQL version 5.0.92

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

•Oracle MySQL >= 5.1 and < 5.1.51

Upgrade to Oracle MySQL version 5.1.51

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

•Oracle MySQL >= 5.5 and < 5.5.6

Upgrade to Oracle MySQL version 5.5.6

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

3.2.282. Oracle MySQL Vulnerability: CVE-2012-0087 (oracle-mysql-cve-2012-0087)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x and 5.1.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0101 and CVE-2012-0102.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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
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.

3.2.283. Oracle MySQL Vulnerability: CVE-2012-0101 (oracle-mysql-cve-2012-0101)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x and 5.1.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0087 and CVE-2012-0102.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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
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.

3.2.284. Oracle MySQL Vulnerability: CVE-2012-0102 (oracle-mysql-cve-2012-0102)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x and 5.1.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0087 and CVE-2012-0101.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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
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.

3.2.285. Oracle MySQL Vulnerability: CVE-2012-0112 (oracle-mysql-cve-2012-0112)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, CVE-2012-0485, and CVE-2012-0492.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0112
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.2.286. Oracle MySQL Vulnerability: CVE-2012-0115 (oracle-mysql-cve-2012-0115)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0119, CVE-2012-0120, CVE-2012-0485, and CVE-2012-0492.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0115
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.2.287. Oracle MySQL Vulnerability: CVE-2012-0117 (oracle-mysql-cve-2012-0117)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0491, CVE-2012-0493, and CVE-2012-0495.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0117
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.2.288. Oracle MySQL Vulnerability: CVE-2012-0119 (oracle-mysql-cve-2012-0119)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0120, CVE-2012-0485, and CVE-2012-0492.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0119
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.2.289. Oracle MySQL Vulnerability: CVE-2012-0120 (oracle-mysql-cve-2012-0120)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0119, CVE-2012-0485, and CVE-2012-0492.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0120
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.2.290. Oracle MySQL Vulnerability: CVE-2012-0484 (oracle-mysql-cve-2012-0484)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows remote authenticated users to affect confidentiality via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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
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.

3.2.291. Oracle MySQL Vulnerability: CVE-2012-0485 (oracle-mysql-cve-2012-0485)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, and CVE-2012-0492.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
BID	51513
CVE	CVE-2012-0485
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72526

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.2.292. Oracle MySQL Vulnerability: CVE-2012-0487 (oracle-mysql-cve-2012-0487)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0488, CVE-2012-0489, CVE-2012-0491, CVE-2012-0493, and CVE-2012-0495.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference

Source	Reference
BID	51503
CVE	CVE-2012-0487
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72528

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.2.293. Oracle MySQL Vulnerability: CVE-2012-0488 (oracle-mysql-cve-2012-0488)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0487, CVE-2012-0489, CVE-2012-0491, CVE-2012-0493, and CVE-2012-0495.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference

Source	Reference
BID	51506
CVE	CVE-2012-0488
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72529

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.2.294. Oracle MySQL Vulnerability: CVE-2012-0489 (oracle-mysql-cve-2012-0489)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0491, CVE-2012-0493, and CVE-2012-0495.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference

Source	Reference
BID	51510
CVE	CVE-2012-0489
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72530

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.2.295. Oracle MySQL Vulnerability: CVE-2012-0490 (oracle-mysql-cve-2012-0490)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows remote authenticated users to affect availability via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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

Source	Reference
CVE	CVE-2012-0490
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.

3.2.296. Oracle MySQL Vulnerability: CVE-2012-0491 (oracle-mysql-cve-2012-0491)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0493, and CVE-2012-0495.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
BID	51518

Source	Reference
CVE	CVE-2012-0491
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72532

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.2.297. Oracle MySQL Vulnerability: CVE-2012-0495 (oracle-mysql-cve-2012-0495)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0491, and CVE-2012-0493.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0495

Source	Reference
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72533

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.2.298. PHP Vulnerability: CVE-2007-4887 (php-cve-2007-4887)

Description:

The dl function in PHP 5.2.4 and earlier allows context-dependent attackers to cause a denial of service (application crash) via a long string in the library parameter. NOTE: there are limited usage scenarios under which this would be a vulnerability.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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

Source	Reference
OVAL	5767

Vulnerability Solution:

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

3.2.299. PHP Vulnerability: CVE-2007-5447 (php-cve-2007-5447)

Description:

ioncube_loader_win_5.2.dll in the ionCube Loader 6.5 extension for PHP 5.2.4 does not follow safe_mode and disable_functions restrictions, which allows context-dependent attackers to bypass intended limitations, as demonstrated by reading arbitrary files via the ioncube_read_file function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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
XF	37227

Vulnerability Solution:

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

3.2.300. PHP Vulnerability: CVE-2007-5899 (php-cve-2007-5899)

Description:

The output_add_rewrite_var function in PHP before 5.2.5 rewrites local forms in which the ACTION attribute references a non-local URL, which allows remote attackers to obtain potentially sensitive information by reading the requests for this URL, as demonstrated by a rewritten form containing a local session ID.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2007-5899
DEBIAN	DSA-1444
OVAL	11211
REDHAT	RHSA-2008:0505
REDHAT	RHSA-2008:0544
REDHAT	RHSA-2008:0545
REDHAT	RHSA-2008:0546
REDHAT	RHSA-2008:0582

Vulnerability Solution:

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

3.2.301. PHP Vulnerability: CVE-2009-2687 (php-cve-2009-2687)

Description:

The exif_read_data function in the Exif module in PHP before 5.2.10 allows remote attackers to cause a denial of service (crash) via a malformed JPEG image with invalid offset fields, a different issue than CVE-2005-3353.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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	35440
CVE	CVE-2009-2687
DEBIAN	DSA-1940
OVAL	10695
OVAL	6655
URL	http://www.php.net/releases/5_2_10.php
XF	51253

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.10.tar.gz

3.2.302. PHP Vulnerability: CVE-2009-4142 (php-cve-2009-4142)

Description:

The htmlspecialchars function in PHP before 5.2.12 does not properly handle (1) overlong UTF-8 sequences, (2) invalid Shift_JIS sequences, and (3) invalid EUC-JP sequences, which allows remote attackers to conduct cross-site scripting (XSS) attacks by placing a crafted byte sequence before a special character.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
BID	37389
CVE	CVE-2009-4142
DEBIAN	DSA-2001
OVAL	10005
OVAL	7085

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

3.2.303. PHP Vulnerability: CVE-2010-3709 (php-cve-2010-3709)

Description:

The ZipArchive::getArchiveComment function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ZIP archive.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
BID	44718
CVE	CVE-2010-3709
REDHAT	RHSA-2011:0195

Vulnerability Solution:

•Upgrade to PHP version 5.2.14

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

•Upgrade to PHP version 5.3.3

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.3.tar.gz

3.2.304. PHP Vulnerability: CVE-2011-0421 (php-cve-2011-0421)

Description:

The _zip_name_locate function in zip_name_locate.c in the Zip extension in PHP before 5.3.6 does not properly handle a ZIPARCHIVE::FL_UNCHANGED argument, which might allow context-dependent attackers to cause a denial of service (NULL pointer dereference) via an empty ZIP archive that is processed with a (1) locateName or (2) statName operation.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2011-10-12-3
BID	46354
CVE	CVE-2011-0421
DEBIAN	DSA-2266
XF	66173

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.6.tar.gz

3.2.305. PHP Vulnerability: CVE-2011-0708 (php-cve-2011-0708)

Description:

exif.c in the Exif extension in PHP before 5.3.6 on 64-bit platforms performs an incorrect cast, which allows remote attackers to cause a denial of service (application crash) via an image with a crafted Image File Directory (IFD) that triggers a buffer over-read.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2011-10-12-3
BID	46365
CVE	CVE-2011-0708
DEBIAN	DSA-2266
REDHAT	RHSA-2011:1423
REDHAT	RHSA-2012:0071

Vulnerability Solution:
Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.6.tar.gz

3.2.306. PHP Vulnerability: CVE-2011-1398 (php-cve-2011-1398)

Description:

The sapi_header_op function in main/SAPI.c in PHP before 5.3.11 and 5.4.x before 5.4.0RC2 does not check for %0D sequences (aka carriage return characters), which allows remote attackers to bypass an HTTP response-splitting protection mechanism via a crafted URL, related to improper interaction between the PHP header function and certain browsers, as demonstrated by Internet Explorer and Google Chrome.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
CVE	CVE-2011-1398

Source	Reference
REDHAT	RHSA-2013:1307

Vulnerability Solution:

•Upgrade to PHP version 5.3.11

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

•Upgrade to PHP version 5.4.0

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

3.2.307. PHP Vulnerability: CVE-2011-1471 (php-cve-2011-1471)

Description:

Integer signedness error in zip_stream.c in the Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (CPU consumption) via a malformed archive file that triggers errors in zip_fread function calls.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2011-10-12-3
BID	46975
CVE	CVE-2011-1471
DEBIAN	DSA-2266
REDHAT	RHSA-2011:1423

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.6.tar.gz

3.2.308. PHP Fixed possible attack in SSL sockets with SSL 3.0 / TLS 1.0 (php-cve-2011-3389)

Description:

The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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
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/

3.2.309. PHP Vulnerability: CVE-2015-8935 (php-cve-2015-8935)

Description:

The sapi_header_op function in main/SAPI.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 supports deprecated line folding without considering browser compatibility, which allows remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer by leveraging (1) %0A%20 or (2) %0D%0A%20 mishandling in the header function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2015-8935
REDHAT	RHSA-2016:2750
URL	https://bugs.php.net/bug.php?id=68978

Vulnerability Solution:

•Upgrade to PHP version 5.4.38

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

•Upgrade to PHP version 5.5.22

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

•Upgrade to PHP version 5.6.6

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

3.2.310. 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:
192.168.234.131:80	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
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/

3.2.311. 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:
192.168.234.131:80	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
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/

3.2.312. PHP Fixed dl() to limit argument size to MAXPATHLEN (php-fixed-dl-to-limit-argument-size-to-maxpathlen)

Description:

The dl function in PHP 5.2.4 and earlier allows context-dependent attackers to cause a denial of service (application crash) via a long string in the library parameter. NOTE: there are limited usage scenarios under which this would be a vulnerability.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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

3.2.313. PHP Fixed NULL pointer dereference in ZipArchive::getArchiveComment (php-fixed-null-pointer-dereference-in-ziparchivegetarchivecomment)

Description:

The ZipArchive::getArchiveComment function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ZIP archive.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
BID	44718
CVE	CVE-2010-3709
REDHAT	RHSA-2011:0195

Vulnerability Solution:

•Upgrade to PHP version 5.2.15

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.15.tar.gz

•Upgrade to PHP version 5.3.4

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

3.2.314. TLS/SSL Server is enabling the BEAST attack (ssl-cve-2011-3389-beast)

Description:

The SSL protocol, as used in certain configurations of Microsoft Windows and browsers such as Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera (and other products negotiating SSL connections) encrypts data by using CBC mode with chained initialization vectors. This potentially 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. By supporting the affected protocols and ciphers, the server is enabling the clients in to being exploited.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:443	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_DHE_RSA_WITH_SEED_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHATLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_RSA_WITH_IDEA_CBC_SHATLS_RSA_WITH_SEED_CBC_SHA

References:

Source	Reference

Source	Reference
CVE	CVE-2011-3389
URL	http://vnhacker.blogspot.co.uk/2011/09/beast.html

Vulnerability Solution:

There is no server-side mitigation available against the BEAST attack. The only option is to disable the affected protocols (SSLv3 and TLS 1.0). The only fully safe configuration is to use Authenticated Encryption with Associated Data (AEAD), e.g. AES-GCM, AES-CCM in TLS 1.2.

3.2.315. 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:
192.168.234.130:443	TLS/SSL certificate is self-signed.
192.168.234.131:5432	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.

3.2.316. 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:
192.168.234.131:5432	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.

3.2.317. Unencrypted Telnet Service Available (telnet-open-port)

Description:

Telnet is an unencrypted protocol, as such it sends sensitive data (usernames, passwords) in clear text.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:23	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.

3.2.318. 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:
192.168.234.130:443	Successfully connected over TLSv1.0
192.168.234.131:5432	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.

3.2.319. VMware Player: Updated OpenSSL library to address various security vulnerabilities (VMSA-2008-0005) (CVE-2006-4339) (vmsa-2008-0005-cve-2006-4339-player)

Description:

OpenSSL before 0.9.7, 0.9.7 before 0.9.7k, and 0.9.8 before 0.9.8c, when using an RSA key with exponent 3, removes PKCS-1 padding before generating a hash, which allows remote attackers to forge a PKCS #1 v1.5 signature that is signed by that RSA key and prevents OpenSSL from correctly verifying X.509 and other certificates that use PKCS #1.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
APPLE	APPLE-SA-2006-11-28
APPLE	APPLE-SA-2007-12-14
BID	19849
BID	22083
BID	28276
CERT	TA06-333A
CERT-VN	845620
CVE	CVE-2006-4339
DEBIAN	DSA-1173
DEBIAN	DSA-1174
OVAL	11656
REDHAT	RHSA-2006:0661

Source	Reference
REDHAT	RHSA-2007:0062
REDHAT	RHSA-2007:0072
REDHAT	RHSA-2007:0073
REDHAT	RHSA-2008:0629
SGI	20060901-01-P
SUSE	SUSE-SA:2006:055
SUSE	SUSE-SA:2006:061
SUSE	SUSE-SA:2007:010
URL	http://www.vmware.com/security/advisories/VMSA-2008-0005.html
XF	28755

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.6

Upgrade to VMware Player version 1.0.6

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.0 and < 2.0.3

Upgrade to VMware Player version 2.0.3

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.320. VMware Workstation: Updated OpenSSL library to address various security vulnerabilities (VMSA-2008-0005) (CVE-2006-4339) (vmsa-2008-0005-cve-2006-4339-workstation)

Description:

OpenSSL before 0.9.7, 0.9.7 before 0.9.7k, and 0.9.8 before 0.9.8c, when using an RSA key with exponent 3, removes PKCS-1 padding before generating a hash, which allows remote attackers to forge a PKCS #1 v1.5 signature that is signed by that RSA key and prevents OpenSSL from correctly verifying X.509 and other certificates that use PKCS #1.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
APPLE	APPLE-SA-2006-11-28
APPLE	APPLE-SA-2007-12-14
BID	19849

Source	Reference
BID	22083
BID	28276
CERT	TA06-333A
CERT-VN	845620
CVE	CVE-2006-4339
DEBIAN	DSA-1173
DEBIAN	DSA-1174
OVAL	11656
REDHAT	RHSA-2006:0661
REDHAT	RHSA-2007:0062
REDHAT	RHSA-2007:0072
REDHAT	RHSA-2007:0073
REDHAT	RHSA-2008:0629
SGI	20060901-01-P
SUSE	SUSE-SA:2006:055
SUSE	SUSE-SA:2006:061
SUSE	SUSE-SA:2007:010
URL	http://www.vmware.com/security/advisories/VMSA-2008-0005.html
XF	28755

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.6

Upgrade to VMware Workstation version 5.5.6

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6 and < 6.0.3

Upgrade to VMware Workstation version 6.0.3

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.2.321. VMware Player: Updated OpenSSL library to address various security vulnerabilities (VMSA-2008-0005) (CVE-2006-4343) (vmsa-2008-0005-cve-2006-4343-player)

Description:

The get_server_hello function in the SSLv2 client code in OpenSSL 0.9.7 before 0.9.7l, 0.9.8 before 0.9.8d, and earlier versions allows remote servers to cause a denial of service (client crash) via unknown vectors that trigger a null pointer dereference.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
APPLE	APPLE-SA-2006-11-28
BID	20246
BID	22083
BID	28276
CERT	TA06-333A
CERT-VN	386964
CVE	CVE-2006-4343
DEBIAN	DSA-1185
DEBIAN	DSA-1195
NETBSD	NetBSD-SA2008-007
OVAL	10207
OVAL	4356
REDHAT	RHSA-2006:0695
REDHAT	RHSA-2008:0629
SGI	20061001-01-P
SUSE	SUSE-SA:2006:058
URL	http://www.vmware.com/security/advisories/VMSA-2008-0005.html
XF	29240

Vulnerability Solution:

•VMware Player >= 1.0 and < 1.0.6

Upgrade to VMware Player version 1.0.6

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 2.0 and < 2.0.3

Upgrade to VMware Player version 2.0.3

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.322. VMware Workstation: Updated OpenSSL library to address various security vulnerabilities (VMSA-2008-0005) (CVE-2006-4343) (vmsa-2008-0005-cve-2006-4343-workstation)

Description:

The get_server_hello function in the SSLv2 client code in OpenSSL 0.9.7 before 0.9.7l, 0.9.8 before 0.9.8d, and earlier versions allows remote servers to cause a denial of service (client crash) via unknown vectors that trigger a null pointer dereference.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
APPLE	APPLE-SA-2006-11-28
BID	20246
BID	22083
BID	28276
CERT	TA06-333A
CERT-VN	386964
CVE	CVE-2006-4343
DEBIAN	DSA-1185
DEBIAN	DSA-1195
NETBSD	NetBSD-SA2008-007
OVAL	10207
OVAL	4356
REDHAT	RHSA-2006:0695
REDHAT	RHSA-2008:0629
SGI	20061001-01-P
SUSE	SUSE-SA:2006:058
URL	http://www.vmware.com/security/advisories/VMSA-2008-0005.html
XF	29240

Vulnerability Solution:

•VMware Workstation >= 5.5 and < 5.5.6

Upgrade to VMware Workstation version 5.5.6

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

•VMware Workstation >= 6 and < 6.0.3

Upgrade to VMware Workstation version 6.0.3

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_0

3.2.323. VMware Player: VMware Tools Local Privilege Escalation on Windows-based guest OS (VMSA-2008-0009) (CVE-2007-5671) (vmsa-2008-0009-cve-2007-5671-player)

Description:

HGFS.sys in the VMware Tools package in VMware Workstation 5.x before 5.5.6 build 80404, VMware Player before 1.0.6 build 80404, VMware ACE before 1.0.5 build 79846, VMware Server before 1.0.5 build 80187, and VMware ESX 2.5.4 through 3.0.2 does not properly validate arguments in user-mode METHOD_NEITHER IOCTLs to the \\.\hgfs device, which allows guest OS users to modify arbitrary memory locations in guest kernel memory and gain privileges.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
CVE	CVE-2007-5671
OVAL	5358
OVAL	5688
URL	http://www.vmware.com/security/advisories/VMSA-2008-0009.html

Vulnerability Solution:

VMware Player >= 1.0 and < 1.0.6
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.324. VMware Workstation: VMware Tools Local Privilege Escalation on Windows-based guest OS (VMSA-2008-0009) (CVE-2007-5671) (vmsa-2008-0009-cve-2007-5671-workstation)

Description:

HGFS.sys in the VMware Tools package in VMware Workstation 5.x before 5.5.6 build 80404, VMware Player before 1.0.6 build 80404, VMware ACE before 1.0.5 build 79846, VMware Server before 1.0.5 build 80187, and VMware ESX 2.5.4 through 3.0.2 does not properly validate arguments in user-mode METHOD_NEITHER IOCTLs to the \\.\hgfs device, which allows guest OS users to modify arbitrary memory locations in guest kernel memory and gain privileges.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
CVE	CVE-2007-5671
OVAL	5358
OVAL	5688
URL	http://www.vmware.com/security/advisories/VMSA-2008-0009.html

Vulnerability Solution:

VMware Workstation >= 5.5 and < 5.5.6
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/5_5

3.2.325. VMware Player: VMware Descheduled Time Accounting driver vulnerability may cause a denial of service in Windows based virtual machines (VMSA-2009-0007) (CVE-2009-1805) (vmsa-2009-0007-cve-2009-1805-player)

Description:

Unspecified vulnerability in the VMware Descheduled Time Accounting driver in VMware Workstation 6.5.1 and earlier, VMware Player 2.5.1 and earlier, VMware ACE 2.5.1 and earlier, VMware Server 1.x before 1.0.9 build 156507 and 2.x before 2.0.1 build 156745, VMware Fusion 2.x before 2.0.2 build 147997, VMware ESXi 3.5, and VMware ESX 3.0.2, 3.0.3, and 3.5, when the Descheduled Time Accounting Service is not running, allows guest OS users on Windows to cause a denial of service via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	35141
CVE	CVE-2009-1805
OVAL	6130
URL	http://www.vmware.com/security/advisories/VMSA-2009-0007.html

Vulnerability Solution:

VMware Player >= 2.5 and < 2.5.2
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.326. VMware Workstation: VMware Descheduled Time Accounting driver vulnerability may cause a denial of service in Windows based virtual machines (VMSA-2009-0007) (CVE-2009-1805) (vmsa-2009-0007-cve-2009-1805-workstation)

Description:

Unspecified vulnerability in the VMware Descheduled Time Accounting driver in VMware Workstation 6.5.1 and earlier, VMware Player 2.5.1 and earlier, VMware ACE 2.5.1 and earlier, VMware Server 1.x before 1.0.9 build 156507 and 2.x before 2.0.1 build 156745, VMware Fusion 2.x before 2.0.2 build 147997, VMware ESXi 3.5, and VMware ESX 3.0.2, 3.0.3, and 3.5, when the Descheduled Time Accounting Service is not running, allows guest OS users on Windows to cause a denial of service via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	35141
CVE	CVE-2009-1805
OVAL	6130
URL	http://www.vmware.com/security/advisories/VMSA-2009-0007.html

Vulnerability Solution:

VMware Workstation >= 6.5 and < 6.5.2
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

3.2.327. VMware Player: Third party library update for libpng to version 1.2.37 (VMSA-2010-0007) (CVE-2009-2042) (vmsa-2010-0007-cve-2009-2042-player)

Description:

libpng before 1.2.37 does not properly parse 1-bit interlaced images with width values that are not divisible by 8, which causes libpng to include uninitialized bits in certain rows of a PNG file and might allow remote attackers to read portions of sensitive memory via "out-of-bounds pixels" in the file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
BID	35233
CVE	CVE-2009-2042

Source	Reference
DEBIAN	DSA-2032
DISA_SEVERITY	Category I
DISA_VMSKEY	V0023997
IAVM	2010-A-0066
URL	http://www.vmware.com/security/advisories/VMSA-2010-0007.html
XF	50966

Vulnerability Solution:

•VMware Player >= 2.5 and < 2.5.4

Upgrade to VMware Player version 2.5.4

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 3.0 and < 3.0.1

Upgrade to VMware Player version 3.0.1

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.328. VMware Workstation: Third party library update for libpng to version 1.2.37 (VMSA-2010-0007) (CVE-2009-2042) (vmsa-2010-0007-cve-2009-2042-workstation)

Description:

libpng before 1.2.37 does not properly parse 1-bit interlaced images with width values that are not divisible by 8, which causes libpng to include uninitialized bits in certain rows of a PNG file and might allow remote attackers to read portions of sensitive memory via "out-of-bounds pixels" in the file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
BID	35233
CVE	CVE-2009-2042
DEBIAN	DSA-2032
DISA_SEVERITY	Category I
DISA_VMSKEY	V0023997
IAVM	2010-A-0066

Source	Reference
URL	http://www.vmware.com/security/advisories/VMSA-2010-0007.html
XF	50966

Vulnerability Solution:

•VMware Workstation >= 6.5 and < 6.5.4

Upgrade to VMware Workstation version 6.5.4

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/6_5

•VMware Workstation >= 7 and < 7.0.1

Upgrade to VMware Workstation version 7.0.1

Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.2.329. VMware Player: OpenSSL update for multiple products (VMSA-2014-0006) (CVE-2010-5298) (vmsa-2014-0006-cve-2010-5298-player)

Description:

Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	66801
CVE	CVE-2010-5298
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052893
DISA_VMSKEY	V0052907
DISA_VMSKEY	V0052909
DISA_VMSKEY	V0052911
DISA_VMSKEY	V0053201
DISA_VMSKEY	V0053319
DISA_VMSKEY	V0053501

Source	Reference
DISA_VMSKEY	V0053505
DISA_VMSKEY	V0053507
IAVM	2014-A-0100
IAVM	2014-A-0115
IAVM	2014-B-0077
IAVM	2014-B-0088
IAVM	2014-B-0089
IAVM	2014-B-0091
IAVM	2014-B-0092
IAVM	2014-B-0097
IAVM	2014-B-0101
IAVM	2014-B-0102
URL	http://www.vmware.com/security/advisories/VMSA-2014-0006.html

Vulnerability Solution:

•VMware Player >= 5.0 and < 5.0.4

Upgrade to VMware Player version 5.0.4

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 6.0 and < 6.0.3

Upgrade to VMware Player version 6.0.3

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.330. VMware Workstation: OpenSSL update for multiple products (VMSA-2014-0006) (CVE-2010-5298) (vmsa-2014-0006-cve-2010-5298-workstation)

Description:

Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference

Source	Reference
BID	66801
CVE	CVE-2010-5298
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052893
DISA_VMSKEY	V0052907
DISA_VMSKEY	V0052909
DISA_VMSKEY	V0052911
DISA_VMSKEY	V0053201
DISA_VMSKEY	V0053319
DISA_VMSKEY	V0053501
DISA_VMSKEY	V0053505
DISA_VMSKEY	V0053507
IAVM	2014-A-0100
IAVM	2014-A-0115
IAVM	2014-B-0077
IAVM	2014-B-0088
IAVM	2014-B-0089
IAVM	2014-B-0091
IAVM	2014-B-0092
IAVM	2014-B-0097
IAVM	2014-B-0101
IAVM	2014-B-0102
URL	http://www.vmware.com/security/advisories/VMSA-2014-0006.html

Vulnerability Solution:

•VMware Workstation >= 10 and < 10.0.3

Upgrade to VMware Workstation version 10.0.3

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

•VMware Workstation >= 9 and < 9.0.4

Upgrade to VMware Workstation version 9.0.4

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/9_0

3.2.331. VMware Player: OpenSSL update for multiple products (VMSA-2014-0006) (CVE-2014-0198) (vmsa-2014-0006-cve-2014-0198-player)

Description:

The do_ssl3_write function in s3_pkt.c in OpenSSL 1.x through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, does not properly manage a buffer pointer during certain recursive calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors that trigger an alert condition.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	67193
CVE	CVE-2014-0198
DEBIAN	DSA-2931
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052641
DISA_VMSKEY	V0052893
DISA_VMSKEY	V0052907
DISA_VMSKEY	V0052909
DISA_VMSKEY	V0052911
DISA_VMSKEY	V0053201
DISA_VMSKEY	V0053319
DISA_VMSKEY	V0053501
DISA_VMSKEY	V0053505
DISA_VMSKEY	V0053507
IAVM	2014-A-0100
IAVM	2014-A-0115
IAVM	2014-B-0077
IAVM	2014-B-0079
IAVM	2014-B-0088

Source	Reference
IAVM	2014-B-0089
IAVM	2014-B-0091
IAVM	2014-B-0092
IAVM	2014-B-0097
IAVM	2014-B-0101
IAVM	2014-B-0102
URL	http://www.vmware.com/security/advisories/VMSA-2014-0006.html

Vulnerability Solution:

•VMware Player >= 5.0 and < 5.0.4

Upgrade to VMware Player version 5.0.4

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 6.0 and < 6.0.3

Upgrade to VMware Player version 6.0.3

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.332. VMware Workstation: OpenSSL update for multiple products (VMSA-2014-0006) (CVE-2014-0198) (vmsa-2014-0006-cve-2014-0198-workstation)

Description:

The do_ssl3_write function in s3_pkt.c in OpenSSL 1.x through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, does not properly manage a buffer pointer during certain recursive calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors that trigger an alert condition.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	67193
CVE	CVE-2014-0198
DEBIAN	DSA-2931
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052641

Source	Reference
DISA_VMSKEY	V0052893
DISA_VMSKEY	V0052907
DISA_VMSKEY	V0052909
DISA_VMSKEY	V0052911
DISA_VMSKEY	V0053201
DISA_VMSKEY	V0053319
DISA_VMSKEY	V0053501
DISA_VMSKEY	V0053505
DISA_VMSKEY	V0053507
IAVM	2014-A-0100
IAVM	2014-A-0115
IAVM	2014-B-0077
IAVM	2014-B-0079
IAVM	2014-B-0088
IAVM	2014-B-0089
IAVM	2014-B-0091
IAVM	2014-B-0092
IAVM	2014-B-0097
IAVM	2014-B-0101
IAVM	2014-B-0102
URL	http://www.vmware.com/security/advisories/VMSA-2014-0006.html

Vulnerability Solution:

•VMware Workstation >= 10 and < 10.0.3

Upgrade to VMware Workstation version 10.0.3

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

•VMware Workstation >= 9 and < 9.0.4

Upgrade to VMware Workstation version 9.0.4

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/9_0

3.2.333. VMware Player: OpenSSL update for multiple products (VMSA-2014-0006) (CVE-2014-0221) (vmsa-2014-0006-cve-2014-0221-player)

Description:

The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	67901
CVE	CVE-2014-0221
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052641
DISA_VMSKEY	V0053201
DISA_VMSKEY	V0057381
IAVM	2014-A-0100
IAVM	2014-A-0172
IAVM	2014-B-0077
IAVM	2014-B-0079
REDHAT	RHSA-2014:1021
URL	http://www.vmware.com/security/advisories/VMSA-2014-0006.html

Vulnerability Solution:

•VMware Player >= 5.0 and < 5.0.4

Upgrade to VMware Player version 5.0.4

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 6.0 and < 6.0.3

Upgrade to VMware Player version 6.0.3

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.334. VMware Workstation: OpenSSL update for multiple products (VMSA-2014-0006) (CVE-2014-0221) (vmsa-2014-0006-cve-2014-0221-workstation)

Description:

The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	67901
CVE	CVE-2014-0221
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052641
DISA_VMSKEY	V0053201
DISA_VMSKEY	V0057381
IAVM	2014-A-0100
IAVM	2014-A-0172
IAVM	2014-B-0077
IAVM	2014-B-0079
REDHAT	RHSA-2014:1021
URL	http://www.vmware.com/security/advisories/VMSA-2014-0006.html

Vulnerability Solution:

•VMware Workstation >= 10 and < 10.0.3

Upgrade to VMware Workstation version 10.0.3

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

•VMware Workstation >= 9 and < 9.0.4

Upgrade to VMware Workstation version 9.0.4

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/9_0

3.2.335. VMware Player: OpenSSL update for multiple products (VMSA-2014-0006) (CVE-2014-3470) (vmsa-2014-0006-cve-2014-3470-player)

Description:

The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	67898
CVE	CVE-2014-3470
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052641
DISA_VMSKEY	V0052893
DISA_VMSKEY	V0052907
DISA_VMSKEY	V0052909
DISA_VMSKEY	V0052911
DISA_VMSKEY	V0053201
DISA_VMSKEY	V0053319
DISA_VMSKEY	V0053501
DISA_VMSKEY	V0053505
DISA_VMSKEY	V0053507
DISA_VMSKEY	V0060737
IAVM	2014-A-0100
IAVM	2014-A-0115
IAVM	2014-B-0077
IAVM	2014-B-0079
IAVM	2014-B-0088
IAVM	2014-B-0089
IAVM	2014-B-0091
IAVM	2014-B-0092

Source	Reference
IAVM	2014-B-0097
IAVM	2014-B-0101
IAVM	2014-B-0102
IAVM	2015-A-0113
URL	http://www.vmware.com/security/advisories/VMSA-2014-0006.html

Vulnerability Solution:

•VMware Player >= 5.0 and < 5.0.4

Upgrade to VMware Player version 5.0.4

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

•VMware Player >= 6.0 and < 6.0.3

Upgrade to VMware Player version 6.0.3

Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.336. VMware Workstation: OpenSSL update for multiple products (VMSA-2014-0006) (CVE-2014-3470) (vmsa-2014-0006-cve-2014-3470-workstation)

Description:

The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	67898
CVE	CVE-2014-3470
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0052641
DISA_VMSKEY	V0052893
DISA_VMSKEY	V0052907
DISA_VMSKEY	V0052909

Source	Reference
DISA_VMSKEY	V0052911
DISA_VMSKEY	V0053201
DISA_VMSKEY	V0053319
DISA_VMSKEY	V0053501
DISA_VMSKEY	V0053505
DISA_VMSKEY	V0053507
DISA_VMSKEY	V0060737
IAVM	2014-A-0100
IAVM	2014-A-0115
IAVM	2014-B-0077
IAVM	2014-B-0079
IAVM	2014-B-0088
IAVM	2014-B-0089
IAVM	2014-B-0091
IAVM	2014-B-0092
IAVM	2014-B-0097
IAVM	2014-B-0101
IAVM	2014-B-0102
IAVM	2015-A-0113
URL	http://www.vmware.com/security/advisories/VMSA-2014-0006.html

Vulnerability Solution:

•VMware Workstation >= 10 and < 10.0.3

Upgrade to VMware Workstation version 10.0.3

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

•VMware Workstation >= 9 and < 9.0.4

Upgrade to VMware Workstation version 9.0.4

Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/9_0

3.2.337. VMware Player: Vulnerability (VMSA-2016-0010) (CVE-2016-5330) (vmsa-2016-0010-cve-2016-5330-player)

Description:

Untrusted search path vulnerability in the HGFS (aka Shared Folders) feature in VMware Tools 10.0.5 in VMware ESXi 5.0 through 6.0, VMware Workstation Pro 12.1.x before 12.1.1, VMware Workstation Player 12.1.x before 12.1.1, and VMware Fusion 8.1.x before 8.1.1 allows local users to gain privileges via a Trojan horse DLL in the current working directory.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	92323
CVE	CVE-2016-5330
DISA_SEVERITY	Category II
IAVM	2016-B-0124
IAVM	2016-B-0125
IAVM	2016-B-0126
IAVM	2016-B-0127
URL	http://www.vmware.com/security/advisories/VMSA-2016-0010.html

Vulnerability Solution:

VMware Player >= 12.1 and < 12.1.1
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.2.338. VMware Workstation: Vulnerability (VMSA-2016-0010) (CVE-2016-5330) (vmsa-2016-0010-cve-2016-5330-workstation)

Description:

Untrusted search path vulnerability in the HGFS (aka Shared Folders) feature in VMware Tools 10.0.5 in VMware ESXi 5.0 through 6.0, VMware Workstation Pro 12.1.x before 12.1.1, VMware Workstation Player 12.1.x before 12.1.1, and VMware Fusion 8.1.x before 8.1.1 allows local users to gain privileges via a Trojan horse DLL in the current working directory.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	92323
CVE	CVE-2016-5330

Source	Reference
DISA_SEVERITY	Category II
IAVM	2016-B-0124
IAVM	2016-B-0125
IAVM	2016-B-0126
IAVM	2016-B-0127
URL	http://www.vmware.com/security/advisories/VMSA-2016-0010.html

Vulnerability Solution:

VMware Workstation >= 12 and < 12.1.1
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_0

3.2.339. VMware Workstation: Vulnerability (VMSA-2018-0008) (CVE-2018-6957) (vmsa-2018-0008-cve-2018-6957-workstation)

Description:

VMware Workstation (14.x before 14.1.1, 12.x) and Fusion (10.x before 10.1.1 and 8.x) contain a denial-of-service vulnerability which can be triggered by opening a large number of VNC sessions. Note: In order for exploitation to be possible on Workstation and Fusion, VNC must be manually enabled.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	103431
CVE	CVE-2018-6957
URL	http://www.vmware.com/security/advisories/VMSA-2018-0008.html

Vulnerability Solution:

VMware Workstation >= 14 and < 14.1.1
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/14_0

3.2.340. 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:
192.168.234.131:6000	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:
192.168.234.131:80	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

Source	Reference
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. Apache HTTPD: mod_proxy_ftp DoS (CVE-2009-3094) (apache-httpd-cve-2009-3094)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy_ftp. Review your web server configuration for validation. A NULL pointer dereference flaw was found in the mod_proxy_ftp module. A malicious FTP server to which requests are being proxied could use this flaw to crash an httpd child process via a malformed reply to the EPSV or PASV commands, resulting in a limited denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2009-3094
DEBIAN	DSA-1934
OVAL	10981
OVAL	8087
SUSE	SUSE-SA:2009:050
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache HTTPD >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.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 < 2.2.14

Upgrade to Apache HTTPD version 2.2.14

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.14.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.

3.3.3. Apache HTTPD: XSS in mod_negotiation when untrusted uploads are supported (CVE-2012-2687) (apache-httpd-cve-2012-2687)

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 XSS for sites which use mod_negotiation and allow untrusted uploads to locations which have MultiViews enabled. Note: This issue is also known as CVE-2008-0455.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of product HTTPD found -- Apache HTTPD 2.2.8

References:

Source	Reference
APPLE	APPLE-SA-2013-09-12-1
BID	55131
CVE	CVE-2012-2687
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061101
IAVM	2015-A-0149
OVAL	18832
OVAL	19539
REDHAT	RHSA-2012:1591

Source	Reference
REDHAT	RHSA-2012:1592
REDHAT	RHSA-2012:1594
REDHAT	RHSA-2013:0130
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.23

Upgrade to Apache HTTPD version 2.2.23

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.3

Upgrade to Apache HTTPD version 2.4.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.3.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.

3.3.4. 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:
192.168.234.131:53	Vulnerable OS: Ubuntu Linux 8.04 Running DNS serviceProduct BIND exists -- BIND 9.4.2Vulnerable version of product BIND found -- BIND 9.4.2
192.168.234.131:53	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.

3.3.5. MySQL HTML Output Script Insertion Vulnerability (mysql-html-output-script-insertion)

Description:

Cross-site scripting (XSS) vulnerability in the command-line client in MySQL 5.0.26 through 5.0.45, and other versions including versions later than 5.0.45, when the --html option is enabled, allows attackers to inject arbitrary web script or HTML by placing it in a database cell, which might be accessed by this client when composing an HTML document. NOTE: as of 20081031, the issue has not been fixed in MySQL 5.0.67.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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-2010-03-29-1
BID	31486
CVE	CVE-2008-4456

Source	Reference
DEBIAN	DSA-1783
OVAL	11456
REDHAT	RHSA-2009:1289
REDHAT	RHSA-2010:0110
URL	http://bugs.mysql.com/bug.php?id=27884
URL	http://www.henlich.de/it-security/mysql-command-line-client-html-injection-vulnerability
XF	45590

Vulnerability Solution:

Oracle MySQL >= 5.1 and < 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.

3.3.6. Oracle MySQL Vulnerability: CVE-2012-0114 (oracle-mysql-cve-2012-0114)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows local users to affect confidentiality and integrity via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0114
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.3.7. PHP Vulnerability: CVE-2008-5814 (php-cve-2008-5814)

Description:

Cross-site scripting (XSS) vulnerability in PHP, possibly 5.2.7 and earlier, when display_errors is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: because of the lack of details, it is unclear whether this is related to CVE-2006-0208.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	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-2008-5814
DEBIAN	DSA-1789
OVAL	10501
REDHAT	RHSA-2009:0350
XF	47496

Vulnerability Solution:

•Upgrade to PHP version 1.99.0

Download and apply the upgrade from: http://museum.php.net/php1/php-1.99.0.tar.gz

•Upgrade to PHP version 2.0.1

Download and apply the upgrade from: http://museum.php.net/php2/php-2.0.1.tar.gz

•Upgrade to PHP version 5.2.8

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

3.3.8. TLS/SSL Server Supports The Use of Static Key Ciphers (ssl-static-key-ciphers)

Description:

The server is configured to support ciphers known as static key ciphers. These ciphers don't support "Forward Secrecy". In the new specification for HTTP/2, these ciphers have been blacklisted.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:443	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_AES_128_CBC_SHATLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_RSA_WITH_IDEA_CBC_SHATLS_RSA_WITH_SEED_CBC_SHATLS 1.1 ciphers: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_RSA_WITH_IDEA_CBC_SHATLS_RSA_WITH_SEED_CBC_SHATLS 1.2 ciphers: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256TLS_RSA_WITH_AES_128_CCM TLS_RSA_WITH_AES_128_CCM_8 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA256TLS_RSA_WITH_AES_256_CCM TLS_RSA_WITH_AES_256_CCM_8 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 TLS_RSA_WITH_SEED_CBC_SHA

References:

Source	Reference
URL	http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295
URL	https://wiki.mozilla.org/Security/Server_Side_TLS
URL	https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Rule_-_Only_Support_Strong_Cryptographic_Ciphers
URL	http://support.microsoft.com/kb/245030/
URL	https://tools.ietf.org/html/rfc7540/

Vulnerability Solution:

Configure the server to disable support for static key cipher suites.
For Microsoft IIS web servers, see Microsoft Knowledgebase article 245030 for instructions on disabling static key cipher suites.
The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.
Refer to your server vendor documentation to apply the recommended cipher configuration:
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

3.3.9. Diffie-Hellman group smaller than 2048 bits (tls-dh-prime-under-2048-bits)

Description:

The TLS server uses a Diffie-Hellman group with a prime modulus of less than 2048 bits in length. Current estimates are that that an academic team can break a 768-bit prime and that a state-level actor can break a 1024-bit prime.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:443	The following SSL/TLS cipher suites use Diffie-Hellman a prime modulus smaller than 2048 bits:TLS 1.0 ciphers: TLS_DHE_RSA_WITH_AES_256_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bitsTLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bits TLS_DHE_RSA_WITH_AES_128_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bitsTLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bits TLS_DHE_RSA_WITH_SEED_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bitsTLS 1.1 ciphers: TLS_DHE_RSA_WITH_AES_256_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bits TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bitsTLS_DHE_RSA_WITH_AES_128_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bits TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bitsTLS_DHE_RSA_WITH_SEED_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bits

References:

Source	Reference
URL	https://weakdh.org/

Vulnerability Solution:

Please refer to this guide to deploying Diffie-Hellman for TLS for instructions on how to configure the server to use 2048-bit or stronger Diffie-Hellman groups with safe primes.

3.3.10. TLS/SSL Server Is Using Commonly Used Prime Numbers (tls-dh-primes)

Description:

The server is using a common or default prime number as a parameter during the Diffie-Hellman key exchange. This makes the secure session vulnerable to a precomputation attack. An attacker can spend a significant amount of time to generate a lookup/rainbow table for a particular prime number. This lookup table can then be used to obtain the shared secret for the handshake and decrypt the session.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:443	The server is using the following commonly used Diffie-Hellman primes: ffffffffffffffffc90fdaa22168c234c4c6628b80dc1cd129024e088a67cc74020bbea63b139b22514a08798e3404ddef9519b3cd3a431b302b0a6df25f14374fe1356d6d51c245e485b576625e7ec6f44c42e9a637ed6b0bff5cb6f406b7edee386bfb5a899fa5ae9f24117c4b1fe649286651ece65381ffffffffffffffff

References:

Source	Reference
URL	https://weakdh.org/
URL	https://www.openssl.org/docs/manmaster/apps/dhparam.html

Vulnerability Solution:

Configure the server to use a randomly generated Diffie-Hellman group. It's recommend that you generate a 2048-bit group. The simplest way of generating a new group is to use OpenSSL:

openssl dhparam -out dhparams.pem 2048

To use the DH parameters in newer versions of Apache (2.4.8 and newer) and OpenSSL 1.0.2 or later, you can directly specify your DH params file as follows:

SSLOpenSSLConfCmd DHParameters "{path to dhparams.pem}"

If you are using Apache with LibreSSL, or Apache 2.4.7 and OpenSSL 0.9.8a or later, you can append the DHparams you generated earlier to the end of your certificate file and reload the configuration.

For other products see the remediation steps suggested by the original researchers.

3.3.11. 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:
192.168.234.130:443	SSL certificate is signed with SHA1withRSA
192.168.234.131:5432	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).

3.3.12. TLS Server Supports TLS version 1.1 (tlsv1_1-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:
192.168.234.130:443	Successfully connected over TLSv1.1

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.

3.3.13. VMware Player: Vulnerability (VMSA-2014-0001) (CVE-2014-1208) (vmsa-2014-0001-cve-2014-1208-player)

Description:

VMware Workstation 9.x before 9.0.1, VMware Player 5.x before 5.0.1, VMware Fusion 5.x before 5.0.1, VMware ESXi 4.0 through 5.1, and VMware ESX 4.0 and 4.1 allow guest OS users to cause a denial of service (VMX process disruption) by using an invalid port.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	64994
CVE	CVE-2014-1208
DISA_SEVERITY	Category I
DISA_VMSKEY	V0041367
DISA_VMSKEY	V0043879
DISA_VMSKEY	V0043880
DISA_VMSKEY	V0043881
IAVM	2013-A-0205
IAVM	2014-B-0008
IAVM	2014-B-0009
IAVM	2014-B-0010
URL	http://www.vmware.com/security/advisories/VMSA-2014-0001.html
XF	90558

Vulnerability Solution:

VMware Player >= 5.0 and < 5.0.1
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.3.14. VMware Workstation: Vulnerability (VMSA-2014-0001) (CVE-2014-1208) (vmsa-2014-0001-cve-2014-1208-workstation)

Description:

VMware Workstation 9.x before 9.0.1, VMware Player 5.x before 5.0.1, VMware Fusion 5.x before 5.0.1, VMware ESXi 4.0 through 5.1, and VMware ESX 4.0 and 4.1 allow guest OS users to cause a denial of service (VMX process disruption) by using an invalid port.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	64994
CVE	CVE-2014-1208
DISA_SEVERITY	Category I
DISA_VMSKEY	V0041367
DISA_VMSKEY	V0043879
DISA_VMSKEY	V0043880
DISA_VMSKEY	V0043881
IAVM	2013-A-0205
IAVM	2014-B-0008
IAVM	2014-B-0009
IAVM	2014-B-0010
URL	http://www.vmware.com/security/advisories/VMSA-2014-0001.html
XF	90558

Vulnerability Solution:

VMware Workstation >= 9 and < 9.0.1
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/9_0

3.3.15. VMware Player: Vulnerability (VMSA-2015-0001) (CVE-2015-1043) (vmsa-2015-0001-cve-2015-1043-player)

Description:

The Host Guest File System (HGFS) in VMware Workstation 10.x before 10.0.5, VMware Player 6.x before 6.0.5, and VMware Fusion 6.x before 6.0.5 and 7.x before 7.0.1 allows guest OS users to cause a guest OS denial of service via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	72337
CVE	CVE-2015-1043
DISA_SEVERITY	Category I
DISA_VMSKEY	V0058535
IAVM	2015-A-0029
URL	http://www.vmware.com/security/advisories/VMSA-2015-0001.html
XF	100934

Vulnerability Solution:

VMware Player >= 6.0 and < 6.0.5
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.3.16. VMware Workstation: Vulnerability (VMSA-2015-0001) (CVE-2015-1043) (vmsa-2015-0001-cve-2015-1043-workstation)

Description:

The Host Guest File System (HGFS) in VMware Workstation 10.x before 10.0.5, VMware Player 6.x before 6.0.5, and VMware Fusion 6.x before 6.0.5 and 7.x before 7.0.1 allows guest OS users to cause a guest OS denial of service via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	72337
CVE	CVE-2015-1043
DISA_SEVERITY	Category I
DISA_VMSKEY	V0058535
IAVM	2015-A-0029
URL	http://www.vmware.com/security/advisories/VMSA-2015-0001.html
XF	100934

Vulnerability Solution:

VMware Workstation >= 10 and < 10.0.5
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

3.3.17. VMware Player: Vulnerability (VMSA-2015-0001) (CVE-2015-1044) (vmsa-2015-0001-cve-2015-1044-player)

Description:

vmware-authd (aka the Authorization process) in VMware Workstation 10.x before 10.0.5, VMware Player 6.x before 6.0.5, and VMware ESXi 5.0 through 5.5 allows attackers to cause a host OS denial of service via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	72336
CVE	CVE-2015-1044
DISA_SEVERITY	Category I
DISA_VMSKEY	V0058513
DISA_VMSKEY	V0058515
DISA_VMSKEY	V0058535
IAVM	2015-A-0029
IAVM	2015-B-0013
IAVM	2015-B-0014
URL	http://www.vmware.com/security/advisories/VMSA-2015-0001.html
XF	100935

Vulnerability Solution:
VMware Player >= 6.0 and < 6.0.5
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.3.18. VMware Workstation: Vulnerability (VMSA-2015-0001) (CVE-2015-1044) (vmsa-2015-0001-cve-2015-1044-workstation)

Description:

vmware-authd (aka the Authorization process) in VMware Workstation 10.x before 10.0.5, VMware Player 6.x before 6.0.5, and VMware ESXi 5.0 through 5.5 allows attackers to cause a host OS denial of service via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	72336
CVE	CVE-2015-1044
DISA_SEVERITY	Category I
DISA_VMSKEY	V0058513
DISA_VMSKEY	V0058515
DISA_VMSKEY	V0058535
IAVM	2015-A-0029
IAVM	2015-B-0013
IAVM	2015-B-0014
URL	http://www.vmware.com/security/advisories/VMSA-2015-0001.html
XF	100935

Vulnerability Solution:

VMware Workstation >= 10 and < 10.0.5
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

3.3.19. 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:
192.168.234.130:443	Length of RSA modulus in X.509 certificate: 1024 bits (less than 2047 bits)
192.168.234.131:5432	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.

3.3.20. Oracle MySQL Vulnerability: CVE-2012-0075 (oracle-mysql-cve-2012-0075)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows remote authenticated users to affect integrity via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	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
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.

3.3.21. Oracle MySQL Vulnerability: CVE-2012-0492 (oracle-mysql-cve-2012-0492)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, and CVE-2012-0485.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference

Source	Reference
BID	51516
CVE	CVE-2012-0492
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72537

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.3.22. Oracle MySQL Vulnerability: CVE-2012-0493 (oracle-mysql-cve-2012-0493)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0491, and CVE-2012-0495.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference

Source	Reference
CVE	CVE-2012-0493
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
XF	72538

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.3.23. Oracle MySQL Vulnerability: CVE-2012-0494 (oracle-mysql-cve-2012-0494)

Description:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows local users to affect availability via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:3306	Running MySQL serviceProduct MySQL exists -- Oracle MySQL 5.0.51a Vulnerable version of product MySQL found -- Oracle MySQL 5.0.51a

References:

Source	Reference
CVE	CVE-2012-0494
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Source	Reference
XF	72540

Vulnerability Solution:

•Oracle MySQL >= 5.0 and < 5.0.95

Upgrade to Oracle MySQL version 5.0.95

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

•Oracle MySQL >= 5.1 and < 5.1.61

Upgrade to Oracle MySQL version 5.1.61

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

•Oracle MySQL >= 5.5 and < 5.5.20

Upgrade to Oracle MySQL version 5.5.20

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

3.3.24. PHP Vulnerability: CVE-2007-6039 (php-cve-2007-6039)

Description:

PHP 5.2.5 and earlier allows context-dependent attackers to cause a denial of service (application crash) via a long string in (1) the domain parameter to the dgettext function, the message parameter to the (2) dcgettext or (3) gettext function, the msgid1 parameter to the (4) dngettext or (5) ngettext function, or (6) the classname parameter to the stream_wrapper_register function. NOTE: this might not be a vulnerability in most web server environments that support multiple threads, unless this issue can be demonstrated for code execution.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.2.8 Vulnerable version of component PHP found -- PHP 5.2.4-2ubuntu5.10

References:

Source	Reference
BID	26426
BID	26428

Source	Reference
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

3.3.25. Files or directories with no real owner or group (unix-unowned-files-or-dirs)

Description:

One or more files or directories without a real owner or group were found on the system. Files and directories have an owner id and group id associated with them. It is possible for a file's owner id or group id to NOT correspond to a real user (in /etc/passwd) or real group (in /etc/group). This can happen when files are owned by users or groups that have been deleted. It can also happen when .tar files from other systems are extracted with certain options. The danger of having a file or directory owned by a non-existent user or group id is that someday, that user or group id could be assigned to a newly created user or group, members of which would be automatically able to access the file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	The following un-owned files were found.

References:

None

Vulnerability Solution:

For each un-owned file or directory on the system, either delete it or "chown" it to a real user and/or group. You can use the following command to find unowned files or directories:
find / -nouser -o -nogroup

3.3.26. VMware Player: VMware Workstation and Player installer security issue (VMSA-2010-0014) (CVE-2010-3277) (vmsa-2010-0014-cve-2010-3277-player)

Description:

The installer in VMware Workstation 7.x before 7.1.2 build 301548 and VMware Player 3.x before 3.1.2 build 301548 renders an index.htm file if present in the installation directory, which might allow local users to trigger unintended interpretation of web script or HTML by creating this file.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
CVE	CVE-2010-3277
URL	http://www.vmware.com/security/advisories/VMSA-2010-0014.html

Vulnerability Solution:

VMware Player >= 3.1 and < 3.1.2
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.3.27. VMware Workstation: VMware Workstation and Player installer security issue (VMSA-2010-0014) (CVE-2010-3277) (vmsa-2010-0014-cve-2010-3277-workstation)

Description:

The installer in VMware Workstation 7.x before 7.1.2 build 301548 and VMware Player 3.x before 3.1.2 build 301548 renders an index.htm file if present in the installation directory, which might allow local users to trigger unintended interpretation of web script or HTML by creating this file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
CVE	CVE-2010-3277
URL	http://www.vmware.com/security/advisories/VMSA-2010-0014.html

Vulnerability Solution:

VMware Workstation >= 7 and < 7.1.2
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.3.28. VMware Player: Multiple vulnerabilities in mount.vmhgfs (VMSA-2011-0009) (CVE-2011-2146) (vmsa-2011-0009-cve-2011-2146-player)

Description:

mount.vmhgfs in the VMware Host Guest File System (HGFS) in VMware Workstation 7.1.x before 7.1.4, VMware Player 3.1.x before 3.1.4, VMware Fusion 3.1.x before 3.1.3, VMware ESXi 3.5 through 4.1, and VMware ESX 3.0.3 through 4.1 allows guest OS users to determine the existence of host OS files and directories via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Player

References:

Source	Reference
BID	48098
CVE	CVE-2011-2146
DISA_SEVERITY	Category I
DISA_VMSKEY	V0028311
IAVM	2011-A-0075
URL	http://www.vmware.com/security/advisories/VMSA-2011-0009.html
XF	67813

Vulnerability Solution:

VMware Player >= 3.1 and < 3.1.4
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.3.29. VMware Workstation: Multiple vulnerabilities in mount.vmhgfs (VMSA-2011-0009) (CVE-2011-2146) (vmsa-2011-0009-cve-2011-2146-workstation)

Description:

mount.vmhgfs in the VMware Host Guest File System (HGFS) in VMware Workstation 7.1.x before 7.1.4, VMware Player 3.1.x before 3.1.4, VMware Fusion 3.1.x before 3.1.3, VMware ESXi 3.5 through 4.1, and VMware ESX 3.0.3 through 4.1 allows guest OS users to determine the existence of host OS files and directories via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable OS: Ubuntu Linux 8.04 Vulnerable software installed: VMware Workstation

References:

Source	Reference

Source	Reference
BID	48098
CVE	CVE-2011-2146
DISA_SEVERITY	Category I
DISA_VMSKEY	V0028311
IAVM	2011-A-0075
URL	http://www.vmware.com/security/advisories/VMSA-2011-0009.html
XF	67813

Vulnerability Solution:

VMware Workstation >= 7 and < 7.1.4
Download and apply the upgrade from: https://my.vmware.com/web/vmware/info/slug/desktop_downloads/vmware_workstation/7_0

3.3.30. VMware Player: Information Disclosure vulnerability in OpenSSL third party library (VMSA-2014-0004) (CVE-2014-0076) (vmsa-2014-0004-cve-2014-0076-player)

Description:

The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Player

References:

Source	Reference
BID	66363
CVE	CVE-2014-0076
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0053201
DISA_VMSKEY	V0060737
IAVM	2014-A-0100
IAVM	2014-B-0077
IAVM	2015-A-0113
URL	http://www.vmware.com/security/advisories/VMSA-2014-0004.html

Vulnerability Solution:

VMware Player >= 6.0 and < 6.0.2
Download and apply the upgrade from: http://www.vmware.com/go/downloadplayer/

3.3.31. VMware Workstation: Information Disclosure vulnerability in OpenSSL third party library (VMSA-2014-0004) (CVE-2014-0076) (vmsa-2014-0004-cve-2014-0076-workstation)

Description:

The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	66363
CVE	CVE-2014-0076
DISA_SEVERITY	Category I
DISA_VMSKEY	V0052625
DISA_VMSKEY	V0053201
DISA_VMSKEY	V0060737
IAVM	2014-A-0100
IAVM	2014-B-0077
IAVM	2015-A-0113
URL	http://www.vmware.com/security/advisories/VMSA-2014-0004.html

Vulnerability Solution:

VMware Workstation >= 10 and < 10.0.2
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0

3.3.32. VMware Workstation: Vulnerability (VMSA-2017-0006) (CVE-2017-4905) (vmsa-2017-0006-cve-2017-4905-workstation)

Description:

VMware ESXi 6.5 without patch ESXi650-201703410-SG, 6.0 U3 without patch ESXi600-201703401-SG, 6.0 U2 without patch ESXi600-201703403-SG, 6.0 U1 without patch ESXi600-201703402-SG, 5.5 without patch ESXi550-201703401-SG; Workstation Pro / Player 12.x prior to 12.5.5; and Fusion Pro / Fusion 8.x prior to 8.5.6 have uninitialized memory usage. This issue may lead to an information leak.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	97164
CVE	CVE-2017-4905
URL	http://www.vmware.com/security/advisories/VMSA-2017-0006.html

Vulnerability Solution:

VMware Workstation >= 12.5 and < 12.5.5
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

3.3.33. VMware Workstation: Vulnerability (VMSA-2017-0015) (CVE-2017-4925) (vmsa-2017-0015-cve-2017-4925-workstation)

Description:

VMware ESXi 6.5 without patch ESXi650-201707101-SG, ESXi 6.0 without patch ESXi600-201706101-SG, ESXi 5.5 without patch ESXi550-201709101-SG, Workstation (12.x before 12.5.3), Fusion (8.x before 8.5.4) contain a NULL pointer dereference vulnerability. This issue occurs when handling guest RPC requests. Successful exploitation of this issue may allow attackers with normal user privileges to crash their VMs.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Vulnerable software installed: VMware Workstation

References:

Source	Reference
BID	100842
CVE	CVE-2017-4925
URL	http://www.vmware.com/security/advisories/VMSA-2017-0015.html

Vulnerability Solution:

VMware Workstation >= 12.5 and < 12.5.3
Download and apply the upgrade from:
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/12_5

3.3.34. 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:
192.168.234.131	Sucessfully read share "tmp" and found the following files:.ICE-unix 5111.jsvc_up.X11-unix.X0-lock#sql1276_3714_0.MYD#sql1276_3714_0.frm #sql1276_3714_0.MYI

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.

3.3.35. 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:
192.168.234.131:53	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.

3.3.36. FTP access with ftp account (ftp-generic-0001)

Description:

Many FTP servers support a default account with the user ID "ftp" and password "ftp". It is best practice to remove default accounts, if possible. For accounts required by the system, the default password should be changed.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:21	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.

3.3.37. FTP access with anonymous account (ftp-generic-0002)

Description:

Many FTP servers support a default account with the user ID "anonymous" and password "ftp@". It is best practice to remove default accounts, if possible. For accounts required by the system, the default password should be changed.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:21	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.

3.3.38. ICMP timestamp response (generic-icmp-timestamp)

Description:

The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services.

In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130	Able to determine remote system time.
192.168.234.131	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).

3.3.39. TCP timestamp response (generic-tcp-timestamp)

Description:

The remote host responded with a TCP timestamp. The TCP timestamp response can be used to approximate the remote host's uptime, potentially aiding in further attacks. Additionally, some operating systems can be fingerprinted based on the behavior of their TCP timestamps.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130	Able to determine system boot time.
192.168.234.131	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.

3.3.40. NetBIOS NBSTAT Traffic Amplification (netbios-nbstat-amplification)

Description:

A NetBIOS NBSTAT query will obtain the status from a NetBIOS-speaking endpoint, which will include any names that the endpoint is known to respond to as well as the device's MAC address for that endpoint. A NBSTAT response is roughly 3x the size of the request, and because NetBIOS utilizes UDP, this can be used to conduct traffic amplification attacks against other assets, typically in the form of distributed reflected denial of service (DRDoS) attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.130:137	Running CIFS Name Service serviceConfiguration item advertised-name-count set to '6' 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.

3.3.41. OpenSSH "X11UseLocalhost" X11 Forwarding Session Hijacking Vulnerability (ssh-openssh-x11uselocalhost-x11-forwarding-session-hijack)

Description:

OpenSSH before 5.1 sets the SO_REUSEADDR socket option when the X11UseLocalhost configuration setting is disabled, which allows local users on some platforms to hijack the X11 forwarding port via a bind to a single IP address, as demonstrated on the HP-UX platform.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131:22	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.

3.3.42. UDP IP ID Zero (udp-ipid-zero)

Description:

The remote host responded with a UDP packet whose IP ID was zero. Normally the IP ID should be set to a unique value and is used in the reconstruction of fragmented packets. Generally this behavior is only seen with systems derived from a Linux kernel, which may allow an attacker to fingerprint the target's operating system.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.234.131	Received UDP packet with IP ID of zero:IPv4 SRC[192.168.234.131] TGT[192.168.234.1] TOS[0] TTL[64] Flags[40] Proto[17] ID[0] FragOff[0] HDR-LENGTH[20] TOTAL-LENGTH[52] CKSUM[58594] UDP SRC-PORT[51094] TGT-PORT[35051] CKSUM[13980] RAW DATA [24]: 3EECE3CA00000001000000000000000 >..... 0000000000000001 .....

Affected Nodes:	Additional Information:

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
192.168.234.130	tcp	139	2	•Windows 7 Ultimate 6.1 •domain: SKIF-PC •password-mode: encrypt •security-mode: user •smb-signing: disabled •smb1-enabled: true
192.168.234.130	tcp	445	2	•Windows 7 Ultimate 6.1 •domain: SKIF-PC •password-mode: encrypt •security-mode: user •smb-signing: disabled •smb1-enabled: true •smb2-enabled: true •smb2-signing: enabled
192.168.234.131	tcp	139	6	•Samba 3.0.20-Debian •domain: METASPLOITABLE •password-mode: encrypt •security-mode: user •smb-signing: disabled •smb1-enabled: true
192.168.234.131	tcp	445	6	•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
192.168.234.130	udp	137	1	•advertised-name-1: SKIF-PC (Computer Name) •advertised-name-2: WORKGROUP (Domain Name) •advertised-name-3: SKIF-PC (File Server Service) •advertised-name-4: WORKGROUP (Browser Service Elections) •advertised-name-5: WORKGROUP (Master Browser) •advertised-name-6: __MSBROWSE__ (Master Browser) •advertised-name-count: 6 •mac-address: 000C290EC557

4.3. DCE Endpoint Resolution

The DCE Endpoint Resolution service, aka Endpoint Mapper, is used on Microsoft Windows systems by Remote Procedure Call (RPC) clients to determine the appropriate port number to connect to for a particular RPC service. This is similar to the portmapper service used on Unix systems.

4.3.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.130	tcp	135	0	

4.4. DCE RPC

4.4.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.130	tcp	1025	0	•interface-uuid: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D •interface-version: 1 •name: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D •object-interface-uuid: 765294BA-60BC-48B8-92E9-89FD77769D91

Device	Protocol	Port	Vulnerabilities	Additional Information
				•protocol-sequence: ncacn_ip_tcp:192.168.234.130[1025]
192.168.234.130	tcp	1026	0	•interface-uuid: 06BBA54A-BE05-49F9-B0A0-30F790261023 •interface-version: 1 •name: Security Center •protocol-sequence: ncacn_ip_tcp:192.168.234.130[1026]
192.168.234.130	tcp	1027	0	•interface-uuid: 12345778-1234-ABCD-EF00-0123456789AC •interface-version: 1 •name: 12345778-1234-ABCD-EF00-0123456789AC •protocol-sequence: ncacn_ip_tcp:192.168.234.130[1027]
192.168.234.130	tcp	1028	0	•interface-uuid: 58E604E8-9ADB-4D2E-A464-3B0683FB1480 •interface-version: 1 •name: AppInfo •protocol-sequence: ncacn_ip_tcp:192.168.234.130[1028]
192.168.234.130	tcp	1029	0	•interface-uuid: 367ABB81-9844-35F1-AD32-98F038001003 •interface-version: 2 •name: 367ABB81-9844-35F1-AD32-98F038001003 •protocol-sequence: ncacn_ip_tcp:192.168.234.130[1029]
192.168.234.130	tcp	1030	0	•interface-uuid: 12345678-1234-ABCD-EF00-0123456789AB •interface-version: 1 •name: IPSec Policy agent endpoint •protocol-sequence: ncacn_ip_tcp:192.168.234.130[1030]

4.5. 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.

4.5.1. Discovered Instances of this Service

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

4.6. 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.

4.6.1. 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.

4.6.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.130	tcp	21	1	•FileZilla FTP Server 0.9.41 beta •ftp.banner: 220-FileZilla Server version 0.9.41 beta •ftp.plaintext.authentication: true
192.168.234.131	tcp	21	2	•vsFTPd 2.3.4 •ftp.banner: 220 (vsFTPd 2.3.4) •ftp.plaintext.authentication: true

4.7. 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.

4.7.1. 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.

4.7.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.130	tcp	80	3	•Apache HTTPD 2.4.29 •OpenSSL: 1.1.0g •PHP: 7.2.1 •http.banner: Apache/2.4.29 (Win32) OpenSSL/1.1.0g PHP/7.2.1 •http.banner.server: Apache/2.4.29 (Win32) OpenSSL/1.1.0g PHP/7.2.1 •http.banner.x-powered-by: PHP/7.2.1
192.168.234.131	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
192.168.234.131	tcp	8180	3	

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

4.8. HTTPS

HTTPS, the HyperText Transfer Protocol over TLS/SSL, is used to exchange multimedia content on the World Wide Web using encrypted (TLS/SSL) connections. Once the TLS/SSL connection is established, the standard HTTP protocol is used. The multimedia files commonly used with HTTP include text, sound, images and video.

4.8.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.130	tcp	443	5	•Apache HTTPD 2.4.29 •OpenSSL: 1.1.0g •PHP: 7.2.1 •http.banner: Apache/2.4.29 (Win32) OpenSSL/1.1.0g PHP/7.2.1 •http.banner.server: Apache/2.4.29 (Win32) OpenSSL/1.1.0g PHP/7.2.1 •http.banner.x-powered-by: PHP/7.2.1 •ssl: true •ssl.cert.chainerror: [Path does not chain with any of the trust anchors] •ssl.cert.issuer.dn: CN=localhost •ssl.cert.key.alg.name: RSA •ssl.cert.key.rsa.modulusBits: 1024 •ssl.cert.not.valid.after: Sat, 09 Nov 2019 01:48:47 EET •ssl.cert.not.valid.before: Wed, 11 Nov 2009 01:48:47 EET •ssl.cert.selfsigned: true •ssl.cert.serial.number: 13098529066745705731 •ssl.cert.sha1.fingerprint: b0238c547a905bfa119c4e8baccaeacf36491ff6 •ssl.cert.sig.alg.name: SHA1withRSA •ssl.cert.subject.dn: CN=localhost •ssl.cert.validchain: false

Device	Protocol	Port	Vulnerabilities	Additional Information
				•ssl.cert.validsignature: true •ssl.cert.version: 1 •ssl.dh.generator.1024: 2 •ssl.dh.prime.1024: ffffffffffffffffc90fdaa22168c234c4c6628b80dc1cd129024e088a67cc74020bbea63b139b22514a08798e3404ddef9519b3cd3a431b302b0a6df25f14374fe13 56d6d51c245e485b576625e7ec6f44c42e9a637ed6b0bff5cb6f406b7edee386bfb5a899fa5ae9f24117c4b1fe649286 651ece65381ffffffffffffffff •ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2 •sslv2: false •sslv3: false •tlsv1_0: true •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.TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA.dh.keysize: 1024 •tlsv1_0.TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA.dh.keysize: 1024 •tlsv1_0.TLS_DHE_RSA_WITH_SEED_CBC_SHA.dh.keysize: 1024 •tlsv1_0.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC

Device	Protocol	Port	Vulnerabilities	Additional Information
				_SHA,TLS_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_DHE_RSA_WITH_SEED_CBC_SHA,TLS_RSA_WITH_SEED_CBC_SHA,TLS_RSA_WITH_IDEA_CBC_SHA •tlsv1_0.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS •tlsv1_1: true •tlsv1_1.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 1024 •tlsv1_1.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 1024 •tlsv1_1.TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA.dh.keysize: 1024 •tlsv1_1.TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA.dh.keysize: 1024 •tlsv1_1.TLS_DHE_RSA_WITH_SEED_CBC_SHA.dh.keysize: 1024 •tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_DHE_RSA_WITH_SEED_CBC_SHA,TLS_RSA_WITH_SEED_CBC_SHA,TLS_RSA_WITH_IDEA_CBC_SHA •tlsv1_1.extensions: RENEGOTIATION_INFO,EC_POINT_

Device	Protocol	Port	Vulnerabilities	Additional Information
				FORMATS •tlsv1_2: true •tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_256_CCM_8,TLS_DHE_RSA_WITH_AES_256_CCM,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_128_CCM_8,TLS_DHE_RSA_WITH_AES_128_CCM,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384,TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256,TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_CCM_8,TLS_RSA_WITH_AES_256_CCM,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CCM_8,TLS_RSA_WITH_AES_128_CCM,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RS

Device	Protocol	Port	Vulnerabilities	Additional Information
				A_WITH_CAMELLIA_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_DHE_RSA_WITH_SEED_CBC_SHA,TLS_RSA_WITH_SEED_CBC_SHA •tlsv1_2.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS

4.9. MySQL

4.9.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.130	tcp	3306	1	•MariaDB •mysql.error: Host '192.168.234.1' is not allowed to connect to this MariaDB server
192.168.234.131	tcp	3306	9	•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:

Device	Protocol	Port	Vulnerabilities	Additional Information
				/usr/share/mysql/charsets/ •collation_connection: latin1_swedish_ci •collation_database: latin1_swedish_ci •collation_server: latin1_swedish_ci •completion_type: 0 •concurrent_insert: 1 •connect_timeout: 5 •datadir: /var/lib/mysql/ •date_format: %Y-%m-%d •datetime_format: %Y-%m-%d %H:%i:%s •default_week_format: 0 •delay_key_write: ON •delayed_insert_limit: 100 •delayed_insert_timeout: 300 •delayed_queue_size: 1000 •div_precision_increment: 4 •engine_condition_pushdown: OFF •expire_logs_days: 10 •flush: OFF •flush_time: 0 •ft_boolean_syntax: + -><()~*:""&| •ft_max_word_len: 84 •ft_min_word_len: 4 •ft_query_expansion_limit: 20 •ft_stopword_file: (built-in) •group_concat_max_len: 1024 •have_archive: YES •have_bdb: NO •have_blackhole_engine: YES •have_compress: YES •have_crypt: YES •have_csv: YES •have_dynamic_loading: YES •have_example_engine: NO •have_federated_engine: YES •have_geometry: YES •have_innodb: YES •have_isam: NO

Device	Protocol	Port	Vulnerabilities	Additional Information
				•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 •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

Device	Protocol	Port	Vulnerabilities	Additional Information
				•innodb_mirrored_log_groups: 1 •innodb_open_files: 300 •innodb_rollback_on_timeout: OFF •innodb_support_xa: ON •innodb_sync_spin_loops: 20 •innodb_table_locks: ON •innodb_thread_concurrency: 8 •innodb_thread_sleep_delay: 10000 •interactive_timeout: 28800 •join_buffer_size: 131072 •keep_files_on_create: OFF •key_buffer_size: 16777216 •key_cache_age_threshold: 300 •key_cache_block_size: 1024 •key_cache_division_limit: 100 •language: /usr/share/mysql/english/ •large_files_support: ON •large_page_size: 0 •large_pages: OFF •lc_time_names: en_US •license: GPL •local_infile: ON •locked_in_memory: OFF •log: OFF •log_bin: OFF •log_bin_trust_function_creators: OFF •log_error: •log_queries_not_using_indexes: OFF •log_slave_updates: OFF •log_slow_queries: OFF •log_warnings: 1 •logging: disabled •long_query_time: 10 •low_priority_updates: OFF •lower_case_file_system: OFF •lower_case_table_names: 0 •max_allowed_packet: 16776192 •max_binlog_cache_size: 4294967295 •max_binlog_size: 104857600 •max_connect_errors: 10

Device	Protocol	Port	Vulnerabilities	Additional Information
				•max_connections: 100 •max_delayed_threads: 20 •max_error_count: 64 •max_heap_table_size: 16777216 •max_insert_delayed_threads: 20 •max_join_size: 18446744073709551615 •max_length_for_sort_data: 1024 •max_prepared_stmt_count: 16382 •max_relay_log_size: 0 •max_seeks_for_key: 4294967295 •max_sort_length: 1024 •max_sp_recursion_depth: 0 •max_tmp_tables: 32 •max_user_connections: 0 •max_write_lock_count: 4294967295 •multi_range_count: 256 •myisam_data_pointer_size: 6 •myisam_max_sort_file_size: 2147483647 •myisam_recover_options: OFF •myisam_repair_threads: 1 •myisam_sort_buffer_size: 8388608 •myisam_stats_method: nulls_unequal •ndb_autoincrement_prefetch_sz: 32 •ndb_cache_check_time: 0 •ndb_connectstring: •ndb_force_send: ON •ndb_use_exact_count: ON •ndb_use_transactions: ON •net_buffer_length: 16384 •net_read_timeout: 30 •net_retry_count: 10 •net_write_timeout: 60 •new: OFF •old_passwords: OFF •open_files_limit: 1024 •optimizer_prune_level: 1 •optimizer_search_depth: 62 •pid_file: /var/run/mysqld/mysqld.pid

Device	Protocol	Port	Vulnerabilities	Additional Information
				•port: 3306 •preload_buffer_size: 32768 •profiling: OFF •profiling_history_size: 15 •protocolVersion: 10 •protocol_version: 10 •query_alloc_block_size: 8192 •query_cache_limit: 1048576 •query_cache_min_res_unit: 4096 •query_cache_size: 16777216 •query_cache_type: ON •query_cache_wlock_invalidate: OFF •query_prealloc_size: 8192 •range_alloc_block_size: 2048 •read_buffer_size: 131072 •read_only: OFF •read_rnd_buffer_size: 262144 •relay_log_purge: ON •relay_log_space_limit: 0 •rpl_recovery_rank: 0 •secure_auth: OFF •secure_file_priv: •server_id: 0 •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

Device	Protocol	Port	Vulnerabilities	Additional Information
				•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 •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

4.10. 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.

4.10.1. Discovered Instances of this Service

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

Device	Protocol	Port	Vulnerabilities	Additional Information
				•program-version: 4

4.11. 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

4.11.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.131	udp	49044	0	•program-number: 100021 •program-version: 4
192.168.234.131	tcp	60389	0	•program-number: 100021 •program-version: 4

4.12. Postgres

4.12.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.131	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 17:07:45 EEST •ssl.cert.not.valid.before: Wed, 17 Mar 2010 16:07:45 EET •ssl.cert.selfsigned: true •ssl.cert.serial.number: 18084549878917544396

Device	Protocol	Port	Vulnerabilities	Additional Information
				•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: f488fd584e49dbcd20b49de49107366b336c380d451d0f7c88b31c7c5b2d8ef6f3c923c043f0a55b188d8ebb558cb85d38d334fd7c175743a31d186cde33212cb52aff3ce1b1294018118d7c84a70a72d686c40319c807297aca950cd9969fabd00a509b0246d3083d66a45d419f9c7cbd894b221926baaba25ec355e92f78c7 •ssl.protocols: sslv3,tlsv1_0 •sslv3: true •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_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES

Device	Protocol	Port	Vulnerabilities	Additional Information
				_256_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_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_AES_128_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA •tlsv1_0.extensions: RENEGOTIATION_INFO •tlsv1_1: false •tlsv1_2: false

4.13. Remote Execution

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

4.13.1. 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).

4.13.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.131	tcp	512	1	•sslv3: false •tlsv1_0: false •tlsv1_1: false •tlsv1_2: false

4.14. 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.

4.14.1. 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).

4.14.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.131	tcp	513	1	•sslv3: false •tlsv1_0: false •tlsv1_1: false •tlsv1_2: false

4.15. 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.

4.15.1. 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).

4.15.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.131	tcp	514	1	

4.16. 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.

4.16.1. 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.

4.16.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.131	tcp	25	0	•Postfix •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 •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

Device	Protocol	Port	Vulnerabilities	Additional Information
				•supports-verify: FALSE •supports-vrfy: true

4.17. 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.

4.17.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.131	tcp	22	2	•OpenBSD OpenSSH 4.7p1 •ssh.banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 •ssh.protocol.version: 2.0 •ssh.rsa.pubkey.fingerprint: 5656240F211DDEA72BAE61B1243D E8F3

4.18. Shell Backdoor

4.18.1. Discovered Instances of this Service

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

4.19. 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.

4.19.1. 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.

4.19.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.131	tcp	23	1	

4.20. 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.

4.20.1. Discovered Instances of this Service

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

4.21. XWindows

4.21.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.131	tcp	6000	1	

4.22. mountd

4.22.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.131	tcp	42884	1	•program-number: 100005 •program-version: 3
192.168.234.131	udp	51094	1	•program-number: 100005 •program-version: 3

4.23. 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.

4.23.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.131	tcp	111	0	•program-number: 100000

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

4.24. status

4.24.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.234.131	udp	45111	0	•program-number: 100024 •program-version: 1
192.168.234.131	tcp	58943	0	•program-number: 100024 •program-version: 1

5. Discovered Users and Groups

5.1. System

5.1.1. 192.168.234.131

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
backup	User	•comment: •user-id: 1068
bin	User	•comment: •user-id: 1004
bind	User	•comment: •user-id: 1210
daemon	User	•comment: •user-id: 1002
dhcp	User	•comment: •user-id: 1202
distccd	User	•comment: •user-id: 1222
ftp	User	•comment: •user-id: 1214
games	User	•comment: •user-id: 1010
gnats	User	•comment: •full-name: Gnats Bug-Reporting System (admin) •user-id: 1082
irc	User	•comment: •full-name: ircd •user-id: 1078
klog	User	•comment:

Account Name	Type	Additional Information
		•user-id: 1206
libuuid	User	•comment: •user-id: 1200
list	User	•comment: •full-name: Mailing List Manager •user-id: 1076
lp	User	•comment: •user-id: 1014
mail	User	•comment: •user-id: 1016
man	User	•comment: •user-id: 1012
msfadmin	User	•comment: •full-name: msfadmin,,, •user-id: 3000
mysql	User	•comment: •full-name: MySQL Server,,, •user-id: 1218
news	User	•comment: •user-id: 1018
nobody	User	•comment: •user-id: 501
postfix	User	•comment: •user-id: 1212
postgres	User	•comment: •full-name: PostgreSQL administrator,,, •user-id: 1216
proftpd	User	•comment: •user-id: 1226
proxy	User	•comment: •user-id: 1026
root	User	•comment: •user-id: 1000
service	User	•comment:

Account Name	Type	Additional Information
		•full-name: ,,, •user-id: 3004
sshd	User	•comment: •user-id: 1208
sync	User	•comment: •user-id: 1008
sys	User	•comment: •user-id: 1006
syslog	User	•comment: •user-id: 1204
telnetd	User	•comment: •user-id: 1224
tomcat55	User	•comment: •user-id: 1220
user	User	•comment: •full-name: just a user,111,, •user-id: 3002
uucp	User	•comment: •user-id: 1020
www-data	User	•comment: •user-id: 1066

5.2. MySQL

5.2.1. 192.168.234.131

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

6. Discovered Databases

6.1. MySQL

6.1.1. 192.168.234.131

- dvwa
- information_schema
- metasploit
- mysql
- owasp10
- tikiwiki
- tikiwiki195

7. Discovered Files and Directories

7.1. 192.168.234.131

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.