

Appendix E - Vulnerability Information

HIGH SEVERITY VULNERABILITIES

Cisco Video Surveillance Manager Multiple Vulnerabilities Prior To 7.0.0 (# 15335)

Severity: High

Description: Multiple vulnerabilities are present in some versions of Cisco Video Surveillance Manager.

Approved Solution: The vendor has released an advisory to address the issue:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130724-vsm>

Reference: CVE-2013-3431

Multiple Vulnerabilities In PHP Prior To Version 5.2.11 (# 7162)

Severity: High

Description: Versions of PHP prior to version 5.2.11 are prone to multiple vulnerabilities.

Approved Solution: The vendor has released patches to address the issues:-

Upgrade to PHP version 5.2.11

http://www.php.net/releases/5_2_11.php

Reference: CVE-2009-3293

MySQL System Table Overwrite Vulnerability (# 6075)

Severity: High

Description: A vulnerability in MySQL may allow for a privilege escalation attack.

Approved Solution: The vendor has made an update available for remediation. More information can be obtained here:

<http://dev.mysql.com/doc/refman/4.1/en/news-4-1-24.html>

Reference: CVE-2007-6304

PHP HTML Entity Encoder Heap Overflow Vulnerability (# 4730)

Severity: High

Description: Buffer overflows in htmlentities() and htmlspecialchars() in PHP 5 through 5.1.6 and PHP 4 through 4.4.4 may result in arbitrary remote code execution.

Approved Solution: Vendor has released PHP 5.2.0 which fixes this issue. For PHP 4 users it is strongly recommended to patch their version of PHP with the following patch until php.net is providing PHP4 updates.

<http://cvs.php.net/viewvc.cgi/php-src/ext/standard/html.c?r1=1.63.2.23.2.2&r2=1.63.2.23.2.3&view=patch>

A package that addresses this vulnerability for PHP version 4.4.4 has been released for Debian.

Reference: CVE-2006-5706

PHP imap_mail_compose() Stack Buffer Overflow Vulnerability (# 8120)

Severity: High

Description: A buffer overflow vulnerability is present in some versions of PHP.

Approved Solution: For PHP 4.x users, upgrade to version 4.4.5 or later.

For PHP 5.x users, upgrade to version 5.2.1 or later.

PHP is available here:

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

Reference: CVE-2007-1825

PHP Malformed URI Request Heap Overflow Code Execution (# 5869)

Severity: High

Description: A vulnerability in PHP may allow for remote code-execution attacks.

Approved Solution: The vendor has made an upgrade, PHP 5.2.6, available for remediation here:

<http://www.php.net/downloads.php#v5>

Reference: CVE-2008-2108

PHP mbstring Extension Buffer Overflow Vulnerability (# 8142)

Severity: High

Description: A buffer overflow vulnerability is present in some versions of PHP.

Approved Solution: Download the latest version of PHP from the following location:

<http://www.php.net>

Reference: CVE-2008-5557

PHP msg_receive() Memory Allocation Integer Overflow Vulnerability (# 7929)

Severity: High

Description: An integer overflow vulnerability is present in some versions of PHP.

Approved Solution: Download the latest version of PHP from the following location:

<http://php.net>

Reference: CVE-2007-1890

PHP Security Multiple Bypass Vulnerabilities (# 3963)

Severity: High

Description: Multiple vulnerabilities in PHP which allow attackers to bypass security restrictions or conduct cross-site scripting attacks.

Approved Solution: Upgrade to the latest version(s) of PHP available from:

<http://www.php.net>

Reference: CVE-2005-3392

PHP sqlite_udf_decode_binary() Buffer Overflow Vulnerability (# 8103)

Severity: High

Description: A buffer overflow vulnerability is present in some versions of PHP.

Approved Solution: For PHP 4.x users, upgrade to version 4.4.7 or later.

For PHP 5.x users, upgrade to version 5.2.3 or later.

PHP is available here:

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

Reference: CVE-2007-1888

PHP sqlite_udf_decode_binary() Buffer Overflow Vulnerability (CVE-2007-1887) (# 8093)

Severity: High

Description: A buffer overflow vulnerability is present in some versions of PHP.

Approved Solution: For PHP 4.x users, upgrade to version 4.4.5 or later.

For PHP 5.x users, upgrade to version 5.2.1 or later.

PHP is available here:

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

Reference: CVE-2007-1887

PHP str_replace() Memory Allocation Vulnerability (# 5213)

Severity: High

Description: A buffer overflow vulnerability in PHP may allow for arbitrary code execution.

Approved Solution: Download the latest version of PHP from the vendor repository or from the following location:

<http://www.php.net/downloads.php>

Reference: CVE-2007-4586

PHP ZipArchive::extractTo() .zip Files Directory Traversal Vulnerability (# 8179)

Severity: High

Description: A directory traversal vulnerability is present in some versions of PHP.

Approved Solution: Download the latest version of PHP from the following location:

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

Reference: CVE-2008-5658

SSHv1 Protocol Enabled (# 878)

Severity: High

Description: The SSH daemon has SSH version 1 protocol support enabled.

Approved Solution: Configure the SSH server to disallow SSHv1 protocol support or upgrade it to the most recent release available.

To disable SSHv1 support for OpenSSH, do the following:

1. Open the file /etc/sshd_config in a standard text editor such as vi.
2. Edit the Protocol configuration line to include only the value 2.
3. Restart the OpenSSH server.

Example:

```
#cat /etc/sshd_config | grep Protocol
Protocol 1,2
```

```
#vi /etc/sshd_config
edit protocol field to read Protocol 2 and save sshd_config
```

```
#cat /etc/sshd_config | grep Protocol
Protocol 2
```

```
Restart the OpenSSH server:
# kill -HUP `cat /var/run/sshd.pid`
```

To upgrade to the most recent release of OpenSSH or SSH.com SSH server, visit www.openssh.com or www.ssh.com.

=====

To configure only SSHv2 support in Cisco IOS use the following commands:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ssh version 2
Router(config)# end
```

Be sure to save the configuration after making this change.

Reference: CVE-2001-0572

Sun MySQL mysql_log Format String Vulnerability (# 6929)

Severity: High

Description: A vulnerability in MySQL may allow for denial of service attacks.

Approved Solution: The vendor has made an update available for remediation. More information can be obtained here:

<http://lists.mysql.com/commits/77637>

Reference: CVE-2009-2446

LOW SEVERITY VULNERABILITIES

test-cgi Program Detected (# 1171)

Severity: Low

Description: The test-cgi program has been detected.

Approved Solution: McAfee is currently unaware of a vendor-supplied patch or update (05/13/2011).

The following workaround is available:

To fix this problem, it is recommended to delete the test.cgi program from the web server. By default, this program is located in the /cgi-bin directory.

Reference: CVE-1999-0070

MEDIUM SEVERITY VULNERABILITIES

Apache HTPasswd User Command Line Argument Buffer Overflow Vulnerability (# 8192)

Severity: Medium

Description: A buffer overflow vulnerability is present in some versions of Apache HTTP server.

Approved Solution: Download the latest version of Apache HTTP Server from the following location:

<http://httpd.apache.org/download.cgi>

Reference: CVE-2007-2693

Apache mod_imap Module Vulnerability (# 5829)

Severity: Medium

Description: A vulnerability exists in Apache that may allow for cross-site scripting attacks.

Approved Solution: The vendor has made an update available for remediation here:

<http://httpd.apache.org/download.cgi>

Sun has patched this vulnerability in Solaris. Please refer to the vendors advisory for patch information:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-233623-1>

Reference: CVE-2008-0005

Apache Mod Status Vulnerability (# 6979)

Severity: Medium

Description: A vulnerability is present in Apache that may allow for cross site scripting attacks.
Approved Solution: For Apache 1.x users, upgrade to version 1.3.39 or later.
For Apache 2.0.x users, upgrade to version 2.0.61 or later.
For Apache 2.2.x users, upgrade to version 2.2.6 or later.

<http://httpd.apache.org/>

Reference: CVE-2006-5752

Apache Prefork MPM Denial of Service Vulnerability (CVE-2007-3304) (# 6913)

Severity: Medium

Description: A vulnerability in Apache may allow for local denial-of-service attacks.

Approved Solution: For Apache 1.x users, upgrade to version 1.3.39 or later.
For Apache 2.0.x users, upgrade to version 2.0.61 or later.
For Apache 2.2.x users, upgrade to version 2.2.6 or later.

<http://httpd.apache.org/>

Reference: CVE-2007-3304

HTTP Server Prone To Slow Denial Of Service Attack (# 12824)

Severity: Medium

Description: A denial of service vulnerability is present in some HTTP servers.

Approved Solution: Upgrade the Apache HTTP Server to the latest version that has "mod_reqtimeout" module support available by default.

Then enable the module "mod_reqtimeout" and configure it to set the timeout and minimum data rate for receiving requests,

An example configuration is as below:

```
<IfModule reqtimeout_module>
  RequestReadTimeout header=10-20,minrate=500
  RequestReadTimeout body=10,minrate=500
</IfModule>
```

http://httpd.apache.org/docs/trunk/mod/mod_reqtimeout.html

For customers who are not ready to use "mod_reqtimeout" module a workaround is to decrease the "Timeout" setting for Apache to 10 seconds or less, instead of the default 5 minutes (300 seconds), in the Apache web server configuration file.

Example:

```
TimeOut 300
```

<https://httpd.apache.org/docs/2.0/mod/core.html#timeout>

Particular considerations have to be taken into account depending on each organization and the type of clients expected to connect to their web servers.

HTTP servers that use the asynchronous I/O technique are not vulnerable to this attack. Some of those servers are: lighttpd, nginx, Apaches experimental event MPM, IIS 6, IIS7, Cherokee, etc.

Reference: CVE-2007-6750

MySQL 5.1.49 Fixes Multiple Vulnerabilities (# 9867)

Severity: Medium

Description: Multiple vulnerabilities are present in some versions of Oracle MySQL.

Approved Solution: This issue has been fixed in MySQL version 5.1.49, download the latest version of Oracle MySQL from the following location:

<http://www.mysql.com>

Reference: CVE-2010-2008

MySQL Access Validation Denial Of Service Vulnerability (# 8188)

Severity: Medium

Description: A denial of service vulnerability is present in some versions of MySQL server.

Approved Solution: Download the latest version of MySQL server from the following location:

<http://dev.mysql.com/downloads/>

Reference: CVE-2007-3780

MySQL Alter Table Function Information Disclosure Vulnerability (# 8191)

Severity: Medium

Description: An information disclosure vulnerability is present in some versions of MySQL server.

Approved Solution: Download the latest version of MySQL server from the following location:

<http://dev.mysql.com/downloads/mysql/>

Reference: CVE-2007-2693

MySQL Bypass Access Restrictions Through Symlink Vulnerability (# 8042)

Severity: Medium

Description: A misconfiguration vulnerability exists in some versions of MySQL Database server which allows malicious remote network traffic with authenticated privileges to bypass intended access restrictions.

Approved Solution: The vendor recommends the following:

1> All users of MySQL 5.0.x upgrade to versions 5.0.89 or above.

2> All users of MySQL 5.1.x upgrade to versions 5.1.42 or above.

3> All users of MySQL 6.0.x upgrade to versions 6.0.9-alpha or above.

Reference: CVE-2008-7247

MySQL Empty Bit-String Literal Denial Of Service (# 6201)

Severity: Medium

Description: A vulnerability in MySQL may allow for denial of service attacks.

Approved Solution: The vendor has made an update available for remediation. More information can be obtained here:

<http://dev.mysql.com/doc/refman/6.0/en/news-6-0-6.html>

<http://dev.mysql.com/doc/refman/6.0/en/news-6-0-6.html>

<http://dev.mysql.com/doc/refman/5.1/en/news-5-1-26.html>

Reference: CVE-2008-3963

MySQL INFORMATION SCHEMA Remote Denial of Service (# 6041)

Severity: Medium

Description: A vulnerability in MySQL may allow for denial of service attacks.

Approved Solution: The vendor has made an update available for remediation. More information can be obtained here:

<http://dev.mysql.com/doc/refman/5.1/en/news-5-1-14.html>

Reference: CVE-2007-3782

MySQL MyISAM Create Table Local Security Bypass (# 5856)

Severity: Medium

Description: A vulnerability in MySQL may allow for security-bypass attacks.

Approved Solution: Update MySQL 4.1.x to 4.1.24 or later, 5.0.x to 5.0.60 or later, 5.1.x to 5.1.24 or later, and 6.0.x to 6.0.5 or later.

Reference: CVE-2008-2079

MySQL MyISAM Table Privilege Checks Bypass Vulnerability (CVE-2008-4098) (# 6718)

Severity: Medium

Description: A vulnerability in MySQL may allow for local users to bypass some privilege checks.

Approved Solution: The vendor has made an update available for remediation. More information can be obtained here:

<http://www.mysql.com/>

Reference: CVE-2008-4098

MySQL mysql change db Vulnerability (# 6031)

Severity: Medium

Description: A vulnerability is present in MySQL that may allow for a privilege escalation attack.

Approved Solution: The vendor has made an update available for remediation. More information can be gained here:

<http://dev.mysql.com/doc/refman/5.1/en/news-5-1-18.html>

Reference: CVE-2007-2693

MySQL RENAME TABLE Vulnerability (# 6030)

Severity: Medium

Description: A vulnerability is present in MySQL that may allow for a privilege escalation attack.

Approved Solution: The vendor has made an update available for remediation. More information can be gained here:

<http://dev.mysql.com/doc/refman/5.1/en/news-5-1-18.html>

Reference: CVE-2007-2693

MySQL Single Row Subselect Vulnerability (# 5077)

Severity: Medium

Description: A vulnerability is present in MySQL that may allow for a denial of service attack.

Approved Solution: The vendor has made an update available for remediation here:

<http://dev.mysql.com/downloads/mysql/5.0.html>

Reference: CVE-2007-2583

MySQL Statements Denial Of Service Vulnerability (CVE-2009-4019) (# 7434)

Severity: Medium

Description: A vulnerability exists in MySQL that may allow for denial of service attacks.

Approved Solution: The vendor has made patches available for remediation.

Upgrade MySQL 5.1.x to 5.1.41

Upgrade MySQL 5.0.x to 5.0.88

Reference: CVE-2009-4019

MySQL X.509 Certificates Spoofing Vulnerability (# 7435)

Severity: Medium

Description: A vulnerability exists in MySQL that may allow for man-in-the-middle attacks.

Approved Solution: The vendor has made patches available for remediation.

MySQL 5.0.x user should upgrade to 5.0.88
MySQL 5.1.x user should upgrade to 5.1.41
Reference: CVE-2009-4028

NTP Mode 7 Request Denial Of Service Vulnerability (# 10796)

Severity: Medium

Description: A denial of service vulnerability is present in some versions of NTP server.

Approved Solution: Upgrade to NTP version 4.2.4p8 or later available at :

<http://www.ntp.org/>

Reference: CVE-2009-3563

OpenSSL EVP VerifyFinal Security Bypass Vulnerability (# 7996)

Severity: Medium

Description: A security bypass vulnerability is present in some versions of OpenSSL.

Approved Solution: The vendor has released OpenSSL version 0.9.8j to correct this vulnerability.

<http://openssl.org/source/>

Reference: CVE-2008-5077

OpenSSL SSL_get_shared_ciphers() Buffer Underflow Vulnerability (# 7990)

Severity: Medium

Description: A denial of service vulnerability is present in some versions of OpenSSL.

Approved Solution: Download the latest version of OpenSSL from the following location:

<http://www.openssl.org/>

Reference: CVE-2007-5135

PHP .htaccess safe mode And open basedir Security Bypass Vulnerability (# 8070)

Severity: Medium

Description: Multiple security bypass vulnerabilities are present in some versions of PHP.

Approved Solution: For PHP 4.x users, upgrade to version 4.4.8 or later.

For PHP 5.x users, upgrade to version 5.2.4 or later.

PHP is available here:

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

Reference: CVE-2007-3378

PHP ext/filter FDF Support Post Bypass Vulnerability (# 8135)

Severity: Medium

Description: A filter bypass vulnerability is present in some versions of PHP.

Approved Solution: Upgrade to PHP 5.2.1 or later available here:

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

Reference: CVE-2007-1452

PHP iconv_substr() Denial Of Service Vulnerability (# 8046)

Severity: Medium

Description: A denial of service vulnerability is present in some versions of PHP.

Approved Solution: Upgrade to PHP 5.2.5 or later available here:

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

Reference: CVE-2007-4783

PHP imageRotate Function Information Disclosure Vulnerability (# 7509)

Severity: Medium

Description: An array index error exists in the imageRotate function in PHP versions 5.2.8 and earlier that could lead to an information disclosure.

Approved Solution: The vendor has released patches to address these vulnerabilities:

http://www.php.net/releases/5_2_9.php

Reference: CVE-2008-5498

PHP mb_send_mail To Argument Header Injection Vulnerability (# 8189)

Severity: Medium

Description: A CRLF injection vulnerability is present in some versions of PHP.

Approved Solution: Download the latest version of PHP from the following location:

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

Reference: CVE-2005-3883

PHP Multiple Iconv Functions Denial Of Service Vulnerability (# 8038)

Severity: Medium

Description: A denial of service vulnerability is present in some versions of PHP.

Approved Solution: Upgrade to PHP 5.2.5 or later available here:

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

Reference: CVE-2007-4840

PHP php_sprintf_appendstring() Remote Integer Overflow Vulnerability (# 7992)

Severity: Medium

Description: An integer overflow vulnerability is present in some versions of PHP.

Approved Solution: Download the latest version of PHP (5.2.6 or later versions) from the following location:

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

Reference: CVE-2008-1384

PHP php_stream_filter_create() Buffer Overflow Vulnerability (# 8125)

Severity: Medium

Description: A buffer overflow vulnerability is present in some versions of PHP.

Approved Solution: Upgrade to PHP 5.2.1 or later available here:

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

Reference: CVE-2007-1824

PHP substr_compare() Integer Overflow Vulnerability (# 8146)

Severity: Medium

Description: An integer overflow vulnerability is present in some versions of PHP.

Approved Solution: Upgrade to PHP 5.2.2 or later available here:

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

Reference: CVE-2007-1375

Web Server Supports Outdated SSLv2 Protocol (# 1858)

Severity: Medium

08/30/13

HP Confidential

Page 28

Description: The Web server supports version 2 of the Secure Sockets Layer (SSL) protocol.

Approved Solution: Configure the server to use SSL version 3.0 or TLS version 1.0.

SSL version 2.0 should be completely disabled. As such, this check will detect web servers with SSLv2 enabled, even though cipher suites have been disabled.

Refer to the server documentation for instructions on configuring the server.

For Microsoft IIS 4.0 - 6.0, refer to <http://support.microsoft.com/?kbid=245030>

The Protocols registry key under the SCHANNEL key is used to control the use of protocols supported by the Schannel.dll file and to restrict the protocols use to the TLS server or TLS client.

To prohibit the use of the protocols other than SSL 3.0 or TLS 1.0, set the DWORD data of the Enabled value to 0x0 in each of the following registry subkeys under the Protocols key:

- SCHANNEL\Protocols\PCT 1.0\Client
- SCHANNEL\Protocols\PCT 1.0\Server
- SCHANNEL\Protocols\SSL 2.0\Client
- SCHANNEL\Protocols\SSL 2.0\Server

If the above keys/values do not exist, please create them with the appropriate DWORD value of 0. Then reboot the system.

Note that Windows 2008 does not support PCT 1.0 protocol, so you will only need to create the last 2 of the above registry keys

For Apache, refer the documentation available at,

http://httpd.apache.org/docs/2.2/ssl/ssl_howto.html
http://httpd.apache.org/docs/2.4/ssl/ssl_howto.html

Web Server Supports Weak SSL Encryption Certificates (# 1859)

Severity: Medium

Description: The host supports weak cipher session keys when negotiating communications using the SSL protocol.

Approved Solution: Enforce the use of 128-bit SSL keys. This may not be possible in all situations because keys distributed by some vendors use 40 bits. This includes certificates from organizations such as VeriSign. When configuring communications using SSL, use the highest key strength possible (Disable SSLv2 and other low encryption ciphers).

To control the ciphers available for Microsoft IIS servers, please read the following KB articles:

<http://support.microsoft.com/kb/187498>
<http://support.microsoft.com/kb/245030/>

To control the ciphers available for Apache HTTPD server, please read the sslcipher suite directive documentation:

http://httpd.apache.org/docs/current/mod/mod_ssl.html#sslcipher suite

For other web servers please contact the web server vendor documentation for configuration details.