

## Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

---

## Product Focus

[Request Tracker for Windows \(WinRT\) by SecureScout Free Edition \(no upgrade\) v3.4.5 beta2](#) - Download Free WinRT v3.4.5 beta2 installer by filling our download form. Size: 34MB

Download Here:

[http://www.netvigilance.com/productdownloads?productname=winrt\\_setup\\_3\\_4\\_5](http://www.netvigilance.com/productdownloads?productname=winrt_setup_3_4_5)

## This Week in Review

Security budgets on the rise in spite of crisis. 2008 data breaches numbers are high. England worried about national security. And US congressman wants House discussion about cybersecurity.

Enjoy reading & Stay safe.

**Call or email netVigilance to get an update on SecureScout.**

**(503) 524 5758 or [sales@netVigilance.com](mailto:sales@netvigilance.com)**

## Top Security News Stories this Week

### • Analyst firm expects security budgets to rise in 2009

Organizations of all sizes are expected to allocate more of their IT budgets to security spending this year compared to 2008, according to two reports released this week by Forrester Research.

In both enterprises and small-to-medium-size businesses (SMBs), IT security budgets should increase, more money should be allocated to new security initiatives and an increased focus should be placed on securing data and meeting business objectives -- rather than complying with regulatory mandates.

"Security is getting a bigger piece of the IT budget pie," Jonathan Penn, the reports' author and Forrester's vice president of tech industry strategy and security, told SCMagazineUS.com on Tuesday.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Analyst-firm-expects-security-budgets-to-rise-in-2009/article/123597/>

## • Data breaches rose sharply in 2008, study says

January 7, 2009 (IDG News Service) More than 35 million data records were breached in 2008 in the U.S., a figure that underscores continuing difficulties in securing information, according to the Identity Theft Resource Center (ITRC).

It documents 656 breaches in 2008 from a range of well-known U.S. companies and government entities, compared to 446 breaches in 2007, a 47% increase. Information about the breaches was collected by tracking media reports and the disclosures companies are required to make by law.

"More companies are revealing that they have had a data breach, either due to laws or public pressure," the ITRC wrote on its Web site. "Our sense is that two things are happening -- the criminal population is stealing more data from companies and that we are hearing more about the breaches."

Computerworld

Full Story :

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9125125&source=rss\\_topic1](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9125125&source=rss_topic1)

## • MI5: Internet phone services a risk to national security

January 8, 2009 (Computerworld UK) Internet telephone services pose a serious threat to Britain's security, the head of MI5 said.

In an interview with the media Wednesday, Evans, director general at MI5 since 2007, said online phone calls posed a "significant detriment to national security" by enabling terrorists to communicate with less risk.

"If we are to maintain our capability, we are going to have to make decisions [on powers to intercept communications] in the next few years," he was reported as saying in the Daily Telegraph. "Because traditional ways are unlikely to work."

Computerworld

Full Story :

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9125378&source=rss\\_topic1](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9125378&source=rss_topic1)

## • Congressman seeks discussion on House cybersecurity

One of two federal lawmakers who disclosed last summer that their office PCs were infiltrated by foreign hackers is calling on House leaders to schedule a special Congressional meeting on cybersecurity.

The bipartisan session would be held to raise awareness of the growing threats posed by cybercriminals, according to a Monday letter from Rep. Frank Wolf, R-Va.

Wolf wrote letters on Monday to House Speaker Nancy Pelosi, House Majority Leader Steny Hoyer, House Rules Committee Chairwoman Louise Slaughter, Minority Leader John Boehner and ranking Republican on the House Rules Committee David Dreier.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Congressman-seeks-discussion-on-House-cybersecurity/article/123665/>

# New Vulnerabilities Tested in SecureScout

## • 16666 Sendmail ruleset parsing buffer overflow Vulnerability

Sendmail is a popular mail server for Unix systems.

A "potential buffer overflow in ruleset parsing" for Sendmail, when using the nonstandard rulesets recipient, final, or mailer-specific envelope recipients, has unknown consequences.

The vulnerability has been reported in version 8.12.9 and prior.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

### References:

\* CONFIRM:

<http://www.sendmail.org/8.12.10.html>

\* MANDRAKE: MDKSA-2003:092

<http://www.mandriva.com/security/advisories?name=MDKSA-2003:092>

\* DEBIAN: DSA-384

<http://www.debian.org/security/2003/dsa-384>

\* REDHAT: RHSA-2003:283

<http://www.redhat.com/support/errata/RHSA-2003-283.html>

\* BUGTRAQ: 20030917 GLSA: sendmail (200309-13)

<http://marc.theaimsgroup.com/?l=bugtraq&m=106383437615742&w=2>

\* BUGTRAQ: 20030919 [OpenPKG-SA-2003.041] OpenPKG Security Advisory (sendmail)

<http://marc.theaimsgroup.com/?l=bugtraq&m=106398718909274&w=2>

\* CERT-VN: VU#108964

<http://www.kb.cert.org/vuls/id/108964>

\* BID: 8649

<http://www.securityfocus.com/bid/8649>

\* OVAL: oval:org.mitre.oval:def:595

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:595>

\* OVAL: oval:org.mitre.oval:def:3606

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3606>

\* XF: sendmail-ruleset-parsing-bo(13216)

<http://xforce.iss.net/xforce/xfdb/13216>

#### CVE Reference:

CVE-2003-0681 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 16667 Sendmail Use-after-free Vulnerability

Sendmail is a popular mail server for Unix systems.

Use-after-free vulnerability in Sendmail allows remote attackers to cause a denial of service (crash) via a long "header line", which causes a previously freed variable to be referenced.

The vulnerability has been reported in version 8.13.8 and prior.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Attack** Risk: **Medium**

#### References:

\* CONFIRM:

<http://www.sendmail.org/releases/8.13.8.html>

\* DEBIAN: DSA-1164

<http://www.debian.org/security/2006/dsa-1164>

\* MANDRIVA: MDKSA-2006:156

<http://www.mandriva.com/security/advisories?name=MDKSA-2006:156>

\* OPENBSD: [3.8] 20060825 010: SECURITY FIX: August 25, 2006

<http://www.openbsd.org/errata38.html#sendmail3>

\* OPENBSD: [3.9] 20060825 005: SECURITY FIX: August 25, 2006

<http://www.openbsd.org/errata.html#sendmail3>

\* VIM: 20060829 Sendmail vendor dispute - CVE-2006-4434 (fwd)

<http://www.atrillion.org/pipermail/vim/2006-August/000999.html>

\* SUNALERT: 102664

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102664-1>

\* SUSE: SUSE-SR:2006:021

[http://www.novell.com/linux/security/advisories/2006\\_21\\_sr.html](http://www.novell.com/linux/security/advisories/2006_21_sr.html)

\* BID: 19714

<http://www.securityfocus.com/bid/19714>

\* FRISRT: ADV-2006-3393

<http://www.frsirt.com/english/advisories/2006/3393>

\* FRISRT: ADV-2006-3994

<http://www.frsirt.com/english/advisories/2006/3994>

\* OSVDB: 28193

<http://www.osvdb.org/28193>

\* SECTRACK: 1016753

<http://securitytracker.com/id?1016753>

\* SECUNIA: 21637

<http://secunia.com/advisories/21637>

\* SECUNIA: 21641

<http://secunia.com/advisories/21641>

\* SECUNIA: 21696

<http://secunia.com/advisories/21696>

\* SECUNIA: 21700

<http://secunia.com/advisories/21700>

\* SECUNIA: 22369  
<http://secunia.com/advisories/22369>  
\* SECUNIA: 21749  
<http://secunia.com/advisories/21749>

#### CVE Reference:

CVE-2006-4434 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18178 Apache mod\_proxy\_balancer balancer\_handler function denial of service

The balancer\_handler function in mod\_proxy\_balancer in the Apache HTTP Server 2.2.0 through 2.2.6, when a threaded Multi-Processing Module is used, allows remote authenticated users to cause a denial of service (child process crash) via an invalid bb variable.

An error in the "mod\_proxy\_balancer" module when handling specially crafted requests while using a threaded Multi-Processing Module, could be exploited by attackers to crash an affected child process, creating a denial of service condition.

The issue has been fixed in version 2.2.8.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS** Risk: **Medium**

#### References:

\* MISC: The Apache HTTP Server Project  
<http://httpd.apache.org/>  
\* BUGTRAQ: 20080110 SecurityReason - Apache2 CSRF, XSS, Memory Corruption and Denial of Service Vulnerability  
<http://www.securityfocus.com/archive/1/archive/1/486169/100/0/threaded>  
\* CONFIRM:  
[http://httpd.apache.org/security/vulnerabilities\\_22.html](http://httpd.apache.org/security/vulnerabilities_22.html)  
\* FEDORA: FEDORA-2008-1695  
<https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00562.html>  
\* FEDORA: FEDORA-2008-1711  
<https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00541.html>  
\* GENTOO: GLSA-200803-19  
<http://security.gentoo.org/glsa/glsa-200803-19.xml>  
\* MANDRIVA: MDVSA-2008:016  
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:016>  
\* REDHAT: RHSA-2008:0008  
<http://www.redhat.com/support/errata/RHSA-2008-0008.html>  
\* REDHAT: RHSA-2008:0009  
<http://www.redhat.com/support/errata/RHSA-2008-0009.html>  
\* SUSE: SUSE-SA:2008:021  
<http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00004.html>  
\* UBUNTU: USN-575-1  
<http://www.ubuntu.com/usn/usn-575-1>  
\* BID: 27236  
<http://www.securityfocus.com/bid/27236>  
\* FRSIRT: ADV-2008-0048  
<http://www.frsirt.com/english/advisories/2008/0048>  
\* SECUNIA: 28526  
<http://secunia.com/advisories/28526>  
\* SECUNIA: 28749  
<http://secunia.com/advisories/28749>  
\* SECUNIA: 28977  
<http://secunia.com/advisories/28977>  
\* SECUNIA: 29348  
<http://secunia.com/advisories/29348>  
\* SECUNIA: 29640  
<http://secunia.com/advisories/29640>  
\* SREASON: 3523  
<http://securityreason.com/securityalert/3523>

#### CVE Reference:

CVE-2007-6422 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18179 Apache Input Validation Hole in mod\_proxy\_ftp Permits Cross-Site Scripting Attacks

The mod\_proxy\_ftp module does not properly filter HTML code from UTF-7 character set user-supplied input before displaying the input. A remote user can create a specially crafted URL that, when loaded by a target user, will cause

arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the Apache software and will run in the security context of that site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user.

The issue has been fixed in versions 2.0.63, and 2.2.8.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

#### References:

- \* MISC: The Apache HTTP Server Project  
<http://httpd.apache.org/>
- \* SREASONRES: 20080110 Apache (mod\_proxy\_ftp) Undefined Charset UTF-7 XSS Vulnerability  
[http://securityreason.com/achievement\\_securityalert/49](http://securityreason.com/achievement_securityalert/49)
- \* BUGTRAQ: 20080110 SecurityReason - Apache (mod\_proxy\_ftp) Undefined Charset UTF-7 XSS Vulnerability  
<http://www.securityfocus.com/archive/1/archive/1/486167/100/0/threaded>
- \* CONFIRM:  
<http://support.avaya.com/elmodocs2/security/ASA-2008-032.htm>
- \* CONFIRM:  
<http://docs.info.apple.com/article.html?artnum=307562>
- \* APPLE: APPLE-SA-2008-03-18  
<http://lists.apple.com/archives/security-announce/2008/Mar/msg00001.html>
- \* FEDORA: FEDORA-2008-1695  
<https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00562.html>
- \* FEDORA: FEDORA-2008-1711  
<https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00541.html>
- \* GENTOO: GLSA-200803-19  
<http://security.gentoo.org/glsa/glsa-200803-19.xml>
- \* MANDRIVA: MDVSA-2008:014  
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:014>
- \* MANDRIVA: MDVSA-2008:015  
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:015>
- \* MANDRIVA: MDVSA-2008:016  
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:016>
- \* REDHAT: RHSA-2008:0004  
<http://www.redhat.com/support/errata/RHSA-2008-0004.html>
- \* REDHAT: RHSA-2008:0005  
<http://www.redhat.com/support/errata/RHSA-2008-0005.html>
- \* REDHAT: RHSA-2008:0006  
<http://www.redhat.com/support/errata/RHSA-2008-0006.html>
- \* REDHAT: RHSA-2008:0007  
<http://www.redhat.com/support/errata/RHSA-2008-0007.html>
- \* REDHAT: RHSA-2008:0008  
<http://www.redhat.com/support/errata/RHSA-2008-0008.html>
- \* REDHAT: RHSA-2008:0009  
<http://www.redhat.com/support/errata/RHSA-2008-0009.html>
- \* SUSE: SUSE-SA:2008:021  
<http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00004.html>
- \* UBUNTU: USN-575-1  
<http://www.ubuntu.com/usn/usn-575-1>
- \* BID: 27234  
<http://www.securityfocus.com/bid/27234>
- \* FRSIRT: ADV-2008-0924  
<http://www.frsirt.com/english/advisories/2008/0924/references>
- \* FRSIRT: ADV-2008-1875  
<http://www.frsirt.com/english/advisories/2008/1875/references>
- \* SECTRACK: 1019185  
<http://www.securitytracker.com/id?1019185>
- \* SECUNIA: 28467  
<http://secunia.com/advisories/28467>
- \* SECUNIA: 28471  
<http://secunia.com/advisories/28471>
- \* SECUNIA: 28526  
<http://secunia.com/advisories/28526>
- \* SECUNIA: 28607  
<http://secunia.com/advisories/28607>
- \* SECUNIA: 28749  
<http://secunia.com/advisories/28749>
- \* SECUNIA: 28977

<http://secunia.com/advisories/28977>

\* SECUNIA: 29348

<http://secunia.com/advisories/29348>

\* SECUNIA: 29420

<http://secunia.com/advisories/29420>

\* SECUNIA: 29640

<http://secunia.com/advisories/29640>

\* SREASON: 3526

<http://securityreason.com/securityalert/3526>

#### CVE Reference:

CVE-2008-0005 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18180 Apache 'mod\_proxy\_ftp' Wildcard Characters Cross-Site Scripting Vulnerability

The Apache 'mod\_proxy\_ftp' module is prone to a cross-site scripting vulnerability because the application fails to properly sanitize user-supplied input.

An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may help the attacker steal cookie-based authentication credentials and launch other attacks.

The issue is fixed in version 2.0.64, and 2.2.10.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

#### References:

\* MISC: The Apache HTTP Server Project

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

\* BUGTRAQ: 20080806 Apache HTTP Server mod\_proxy\_ftp Wildcard Characters Cross-Site Scripting

<http://www.securityfocus.com/archive/1/archive/1/495180/100/0/threaded>

\* MISC:

<http://www.rapid7.com/advisories/R7-0033>

\* CONFIRM:

<http://svn.apache.org/viewvc?view=rev&revision=682868>

\* CONFIRM:

<http://svn.apache.org/viewvc?view=rev&revision=682871>

\* CONFIRM:

<http://svn.apache.org/viewvc?view=rev&revision=682870>

\* AIXAPAR: PK70197

<http://www-1.ibm.com/support/docview.wss?uid=swg1PK70197>

\* AIXAPAR: PK70937

<http://www-1.ibm.com/support/docview.wss?uid=swg1PK70937>

\* MANDRIVA: MDVSA-2008:194

<http://www.mandriva.com/security/advisories?name=MDVSA-2008:194>

\* MANDRIVA: MDVSA-2008:195

<http://www.mandriva.com/security/advisories?name=MDVSA-2008:195>

\* CERT-VN: VU#663763

<http://www.kb.cert.org/vuls/id/663763>

\* BID: 30560

<http://www.securityfocus.com/bid/30560>

\* FRSIRT: ADV-2008-2315

<http://www.frsirt.com/english/advisories/2008/2315>

\* FRSIRT: ADV-2008-2461

<http://www.frsirt.com/english/advisories/2008/2461>

\* SECTRAK: 1020635

<http://www.securitytracker.com/id?1020635>

\* SECUNIA: 31384

<http://secunia.com/advisories/31384>

\* SECUNIA: 31673

<http://secunia.com/advisories/31673>

#### CVE Reference:

CVE-2008-2939 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18181 PHP php\_admin\_value or php\_admin\_flag protection mechanisms bypass Vulnerability

PHP before 5.2.5 allows local users to bypass protection mechanisms configured through php\_admin\_value or php\_admin\_flag in httpd.conf by using ini\_set to modify arbitrary configuration variables, a different issue than CVE-2006-4625.

The vulnerability has been fixed in PHP version 5.2.5.

Test Case Impact: **Attack** Vulnerability Impact: **Attack** Risk: **Medium**

#### References:

- \* MISC: Remote File Inclusion  
[http://en.wikipedia.org/wiki/Remote\\_File\\_Inclusion](http://en.wikipedia.org/wiki/Remote_File_Inclusion)
- \* MISC: Remote file inclusion vulnerabilities  
<http://lwn.net/Articles/203904/>
- \* CONFIRM:  
<http://bugs.php.net/bug.php?id=41561>
- \* CONFIRM:  
<http://www.php.net/ChangeLog-5.php#5.2.5>
- \* CONFIRM:  
[http://www.php.net/releases/5\\_2\\_5.php](http://www.php.net/releases/5_2_5.php)
- \* CONFIRM:  
<https://issues.rpath.com/browse/RPL-1943>
- \* HP: HPSBUX02332  
<http://www.securityfocus.com/archive/1/archive/1/491693/100/0/threaded>
- \* SECTRAK: 1018934  
<http://securitytracker.com/id?1018934>
- \* SECUNIA: 27648  
<http://secunia.com/advisories/27648>
- \* SECUNIA: 27659  
<http://secunia.com/advisories/27659>
- \* SECUNIA: 30040  
<http://secunia.com/advisories/30040>

#### CVE Reference:

CVE-2007-5900 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18182 PHP htmlentities and htmlspecialchars functions accepting partial multibyte sequences Vulnerability

The (1) htmlentities and (2) htmlspecialchars functions in PHP before 5.2.5 accept partial multibyte sequences, which has unknown impact and attack vectors, a different issue than CVE-2006-5465.

The issue has been solved in PHP version 5.2.5.

Test Case Impact: **Attack** Vulnerability Impact: **Attack** Risk: **High**

#### References:

- \* MISC: Remote File Inclusion  
[http://en.wikipedia.org/wiki/Remote\\_File\\_Inclusion](http://en.wikipedia.org/wiki/Remote_File_Inclusion)
- \* MISC: Remote file inclusion vulnerabilities  
<http://lwn.net/Articles/203904/>
- \* CONFIRM:  
<http://www.php.net/ChangeLog-5.php#5.2.5>
- \* CONFIRM:  
[http://www.php.net/releases/5\\_2\\_5.php](http://www.php.net/releases/5_2_5.php)
- \* CONFIRM:  
<https://issues.rpath.com/browse/RPL-1943>
- \* CONFIRM:  
<https://launchpad.net/bugs/173043>
- \* DEBIAN: DSA-1444  
<http://www.debian.org/security/2008/dsa-1444>
- \* FEDORA: FEDORA-2008-3864  
<https://www.redhat.com/archives/fedora-package-announce/2008-June/msg00773.html>
- \* HP: HPSBUX02332  
<http://www.securityfocus.com/archive/1/archive/1/491693/100/0/threaded>
- \* MANDRIVA: MDVSA-2008:125  
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:125>
- \* MANDRIVA: MDVSA-2008:126  
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:126>
- \* MANDRIVA: MDVSA-2008:127  
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:127>
- \* REDHAT: RHSA-2008:0505  
<http://www.redhat.com/support/errata/RHSA-2008-0505.html>

\* REDHAT: RHSA-2008:0544  
<http://www.redhat.com/support/errata/RHSA-2008-0544.html>  
\* REDHAT: RHSA-2008:0545  
<http://www.redhat.com/support/errata/RHSA-2008-0545.html>  
\* REDHAT: RHSA-2008:0546  
<http://www.redhat.com/support/errata/RHSA-2008-0546.html>  
\* REDHAT: RHSA-2008:0582  
<http://www.redhat.com/support/errata/RHSA-2008-0582.html>  
\* SUSE: SUSE-SA:2008:004  
<http://lists.opensuse.org/opensuse-security-announce/2008-01/msg00006.html>  
\* UBUNTU: USN-549-1  
<http://www.ubuntu.com/support/documentation/usn/usn-549-1>  
\* UBUNTU: USN-549-2  
<http://www.ubuntu.com/usn/usn-549-2>  
\* UBUNTU: USN-628-1  
<http://www.ubuntu.com/usn/usn-628-1>  
\* SECTRAK: 1018934  
<http://securitytracker.com/id?1018934>  
\* SECUNIA: 27648  
<http://secunia.com/advisories/27648>  
\* SECUNIA: 27659  
<http://secunia.com/advisories/27659>  
\* SECUNIA: 27864  
<http://secunia.com/advisories/27864>  
\* SECUNIA: 28249  
<http://secunia.com/advisories/28249>  
\* SECUNIA: 28658  
<http://secunia.com/advisories/28658>  
\* SECUNIA: 30040  
<http://secunia.com/advisories/30040>  
\* SECUNIA: 30828  
<http://secunia.com/advisories/30828>  
\* SECUNIA: 31119  
<http://secunia.com/advisories/31119>  
\* SECUNIA: 31124  
<http://secunia.com/advisories/31124>  
\* SECUNIA: 31200  
<http://secunia.com/advisories/31200>

#### CVE Reference:

CVE-2007-5898 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18185 OpenSSL SSLv2 Client\_Master\_Key Remote Denial Of Service Vulnerability

OpenSSL 0.9.6e uses assertions when detecting buffer overflow attacks instead of less severe mechanisms, which allows remote attackers to cause a denial of service (crash) via certain messages that cause OpenSSL to abort from a failed assertion, as demonstrated using SSLv2 CLIENT\_MASTER\_KEY messages, which are not properly handled in s2\_srvr.c.

The issue has been fixed in version 0.9.6f.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS** Risk: **Medium**

#### References:

\* CONFIRM:  
<http://cvs.openssl.org/chngview?cn=7659>  
\* BUGTRAQ: 20031002 New OpenSSL remote vulnerability (issue date 2003/10/02)  
<http://marc.theaimsgroup.com/?l=bugtraq&m=106511018214983>

#### CVE Reference:

CVE-2002-1568 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18187 Multiple Multicast Vulnerabilities in Cisco IOS Software (cisco-sa-20080924-multicast)

Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS Software that may lead to a denial of service (DoS) condition. Devices that run Cisco IOS Software and are configured for PIM are affected by the first vulnerability. Only Cisco 12000 Series (GSR) routers that are configured for PIM are affected by the second vulnerability.

Available PIM modes on a Cisco IOS device are dense mode, sparse mode, or sparse-dense mode. The mode

determines how the device populates its multicast routing table and how multicast packets are forwarded. PIM must be enabled in one of these modes on at least one interface in order for a device to process IP multicast routing.

Note: There is no default mode setting. Multicast routing is disabled by default. However, a Cisco IOS device is vulnerable if at least one interface is configured for PIM.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS** Risk: **High**

#### References:

- \* CISCO: 20080924 Multiple Multicast Vulnerabilities in Cisco IOS Software  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080a01491.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080a01491.shtml)
- \* CONFIRM:  
<http://tools.cisco.com/security/center/viewAlert.x?alertId=16638>

#### CVE Reference:

- CVE-2008-3808 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))
- CVE-2008-3809 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18193 Cisco uBR10012 Series Devices SNMP Vulnerability (cisco-sa-20080924-ubr)

Cisco uBR10012 series devices need to communicate with an RF Switch when configured for linecard redundancy. This communication is based on SNMP (Simple Network Management Protocol). When linecard redundancy is enabled on a Cisco uBR10012 series device, SNMP is also automatically enabled with a default community string of private that has read/write privileges. Since there are no access restrictions on this community string, it may be exploited by an attacker to gain complete control of the device.

Changing the default community string, adding access restrictions on SNMP or doing both will mitigate this vulnerability. The recommended mitigation is to do both.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

#### References:

- \* CISCO: 20080924 Cisco uBR10012 Series Devices SNMP Vulnerability  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080a014b1.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080a014b1.shtml)

#### CVE Reference:

- CVE-2008-3807 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

#### • CVE-2008-0067 HP CVSS 2.0 Score = 10.0

Multiple stack-based buffer overflows in HP OpenView Network Node Manager (OV NNM) 7.51 allow remote attackers to execute arbitrary code via (1) long string parameters to the OpenView5.exe CGI program; (2) a long string parameter to the OpenView5.exe CGI program, related to ov.dll; or a long string parameter to the (3) getcvdata.exe, (4) ovlaunch.exe, or (5) Toolbar.exe CGI program.

Test Case Impact: Vulnerability Impact: Risk: **High**

#### References:

- BID: <http://www.securityfocus.com/bid/33147>
- BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/499826/100/0/threaded>
- SECTRAK: <http://securitytracker.com/id?1021521>
- MISC: [http://secunia.com/secunia\\_research/2008-13/](http://secunia.com/secunia_research/2008-13/)
- SECUNIA: <http://secunia.com/advisories/28074>

#### CVE Reference: [CVE-2008-0067](http://cve.mitre.org)

#### • CVE-2008-5844 PHP CVSS 2.0 Score = 7.5

PHP 5.2.7 contains an incorrect change to the FILTER\_UNSAFE\_RAW functionality, and unintentionally disables magic\_quotes\_gpc regardless of the actual magic\_quotes\_gpc setting, which might make it easier for context-dependent attackers to conduct SQL injection attacks and unspecified other attacks.

Test Case Impact: Vulnerability Impact: Risk: **High**

**References:**

SECTRAK: <http://www.securitytracker.com/id?1021393>

CONFIRM: <http://www.php.net/ChangeLog-5.php#5.2.8>

CONFIRM: <http://www.php.net/archive/2008.php#id2008-12-08-1>

CONFIRM: <http://www.php.net/archive/2008.php#id2008-12-07-1>

CONFIRM: <http://bugs.php.net/bug.php?id=42718>

**CVE Reference:** [CVE-2008-5844](#)

• **CVE-2008-3819 Cisco CVSS 2.0 Score = 5.0**

dnsserver in Cisco Application Control Engine Global Site Selector (GSS) before 3.0(1) allows remote attackers to cause a denial of service (daemon crash) via a series of crafted DNS requests, aka Bug ID CSCsj70093.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

**References:**

CISCO: [http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080a57481.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080a57481.shtml)

XF: <http://xforce.iss.net/xforce/xfdb/47787>

BID: <http://www.securityfocus.com/bid/33152>

SECTRAK: <http://securitytracker.com/id?1021530>

**CVE Reference:** [CVE-2008-3819](#)

• **CVE-2009-0065 Linux CVSS 2.0 Score = 10.0**

Buffer overflow in net/sctp/sm\_statefuns.c in the Stream Control Transmission Protocol (sctp) implementation in the Linux kernel before 2.6.28-git8 allows remote attackers to have an unknown impact via an FWD-TSN (aka FORWARD-TSN) chunk with a large stream ID.

Test Case Impact: Vulnerability Impact: Risk: **High**

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=478800](https://bugzilla.redhat.com/show_bug.cgi?id=478800)

BID: <http://www.securityfocus.com/bid/33113>

MLIST: <http://www.openwall.com/lists/oss-security/2009/01/05/1>

FRSIRT: <http://www.frsirt.com/english/advisories/2009/0029>

CONFIRM: <http://patchwork.ozlabs.org/patch/15024/>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=9fcb95a105758b81ef0131cd18e2db5149f13e95>

**CVE Reference:** [CVE-2009-0065](#)

• **CVE-2009-0046 Sun CVSS 2.0 Score = 5.0**

Sun GridEngine 5.3 and earlier does not properly check the return value from the OpenSSL EVP\_VerifyFinal 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.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

**References:**

MISC: <http://www.ocert.org/advisories/ocert-2008-016.html>

**CVE Reference:** [CVE-2009-0046](#)

• **CVE-2009-0069 Sun CVSS 2.0 Score = 4.9**

Unspecified vulnerability in the nfs4rename\_persistent\_fh function in the NFS 4 (aka NFSv4) client in the kernel in Sun Solaris 10 and OpenSolaris before snv\_102 allows local users to cause a denial of service (recursive mutex\_enter and panic) via unspecified vectors.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

**References:**

CONFIRM: <http://sunsolve.sun.com/search/document.do?assetkey=1-21-139466-02-1>

XF: <http://xforce.iss.net/xforce/xfdb/47750>

BID: <http://www.securityfocus.com/bid/33128>

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-66-248566-1>

SECUNIA: <http://secunia.com/advisories/33361>

MLIST: <http://mail.opensolaris.org/pipermail/onnv-notify/2008-October/015342.html>

**CVE Reference:** [CVE-2009-0069](#)

• **CVE-2008-4827 Sap CVSS 2.0 Score = 9.3**

Multiple heap-based buffer overflows in the AddTab method in the (1) Tab and (2) CTab ActiveX controls in c1sizer.ocx and the (3) TabOne ActiveX control in sizerone.ocx in ComponentOne SizerOne 8.0.20081.140, as used in ComponentOne Studio for ActiveX 2008, TSC2 Help Desk 4.1.8, SAP GUI 6.40 Patch 29 and 7.10, and possibly other products, allow remote attackers to execute arbitrary code by adding many tabs, or adding tabs with long tab captions.

Test Case Impact: Vulnerability Impact: Risk: **High**

**References:**

XF: <http://xforce.iss.net/xforce/xfdb/47771>

XF: <http://xforce.iss.net/xforce/xfdb/47770>

XF: <http://xforce.iss.net/xforce/xfdb/47769>

BID: <http://www.securityfocus.com/bid/33148>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/499830/100/0/threaded>

SECTRACK: <http://securitytracker.com/id?1021529>

MISC: [http://secunia.com/secunia\\_research/2008-54/](http://secunia.com/secunia_research/2008-54/)

MISC: [http://secunia.com/secunia\\_research/2008-53/](http://secunia.com/secunia_research/2008-53/)

MISC: [http://secunia.com/secunia\\_research/2008-52/](http://secunia.com/secunia_research/2008-52/)

SECUNIA: <http://secunia.com/advisories/32672>

SECUNIA: <http://secunia.com/advisories/32648>

SECUNIA: <http://secunia.com/advisories/32609>

**CVE Reference:** [CVE-2008-4827](#)

• **CVE-2008-5872 Nortel CVSS 2.0 Score = 7.8**

Multiple unspecified vulnerabilities in the UNIStim File Transfer Protocol (UFTP) processing in IP Client Manager (IPCM) in Nortel Multimedia Communication Server (MSC) 5100 3.0.13 allow remote attackers to cause a denial of service (device outage) via a UFTP message that has a negative block size or other crafted Connection Details values.

Test Case Impact: Vulnerability Impact: Risk: **High**

**References:**

XF: <http://xforce.iss.net/xforce/xfdb/45751>

BID: <http://www.securityfocus.com/bid/31633>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/2779>

MISC: <http://voipshield.com/research-details.php?id=120>

CONFIRM: <http://support.nortel.com/go/main.jsp?cscat=BLTNDETAIL&id=774845>

SECUNIA: <http://secunia.com/advisories/32203>

**CVE Reference:** [CVE-2008-5872](https://cve.mitre.org/cve/2008/5872)

### **Vulnerability Resource**

Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the 'security portal for information system security professionals' is well founded. <http://www.infosyssec.org/infosyssec/>

### **Thank You**

Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at [ScoutNews@netVigilance.com](mailto:ScoutNews@netVigilance.com)

### **About SecureScout**

SecureScout is a leading vulnerability scanner and management tool developed and marketed worldwide by NexantiS Corporation.

SecureScout is a trademark of NexantiS Corporation.

netVigilance, Inc. is a partner of NexantiS and an authorized distributor of SecureScout.

### **For any inquiry about SecureScout by:**

Customers in America and Northern Europe contact us at [info@netVigilance.com](mailto:info@netVigilance.com)

Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at [info-scanner@securescout.net](mailto:info-scanner@securescout.net)