

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

[Mydoom Worm Scanner](#) - The S4 MyDoom Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any have been infected by the MyDoom email virus or its variants.

Download Here:

<http://www.netvigilance.com/productdownloads?productname=mydoomwormscanner>

This Week in Review

Payment processors will pay some merchants' fines. Infected Websites currently the biggest threats. Biometrics on the way in the US. Malware may hit record this year.

Enjoy reading & Stay safe.

Call or email netVigilance to get an update on SecureScout.

(503) 524 5758 or sales@netvigilance.com

Top Security News Stories this Week

• Companies offer to pay breach fines

Two credit-card payment processors are offering to cover merchants' fines and penalties in the event of a data breach.

However, the two companies, Heartland Payment Systems and Mercury Payment Systems, have different requirements that must be met before a merchant would qualify for coverage.

For Mercury, the retailer would have to prove it was Payment Card Industry Data Security Standard-compliant (PCI DSS) at the time of a breach. SC Magazine

Full Story :

<http://www.scmagazineus.com/Companies-offer-to-pay-breach-fines/article/140350/>

• Every 3.6 seconds a website is infected

Infected websites have been the single biggest threat over the past six months, and the threat vectors that have seen the most growth are Web 2.0 and social networking technologies, according to the report, which was released

Wednesday by security firm Sophos.

Approximately 23,500 infected webpages are discovered every day - that's a new one every 3.6 seconds, according to Sophos' recently released July security threat report. That infection rate is faster than in 2008, during which the first half of that year saw a newly infected website being identified every 4.5 seconds, Richard Wang, manager, Sophos Labs U.S. told SCMagazineUS.com on Tuesday.

"Compromised sites are the threat that people are most likely to encounter," Wang said. SC Magazine

Full Story :

<http://www.scmagazineus.com/Every-36-seconds-a-website-is-infected/article/140414/>

• Congress eyes biometric authentication for job eligibility

Computerworld - In a move likely to heighten concerns among opponents of a national ID card, some lawmakers are proposing that biometrics be used to authenticate the identity of anyone seeking a job in the U.S.

At a hearing by the Senate Judiciary Committee's Subcommittee on Immigration, Border Security and Citizenship, lawmakers from both parties expressed broad support Tuesday for strengthening the E-Verify online employment eligibility verification program with biometrics.

The chairman of the subcommittee, Sen. Charles Schumer, (D-N.Y.), said that E-Verify only checks whether the name, date of birth, citizenship status and other details provided by a job applicant match those in official records from the Social Security Administration and the IRS. The process does little to stop identity thieves and those using identity credentials fraudulently from working illegally in the U.S. Computerworld

Full Story :

http://www.computerworld.com/s/article/9135820/Congress_eyes_biometric_authentication_for_job_eligibility?source=rss

• Malware pace quickens dramatically

During the first half of the year, more than 1.2 million unique samples of malware hit the web. That is well ahead of the pace of last year and could put this year in the record books, according to research by McAfee Avert Labs.

"In the first half of 2009, we have seen three times the unique malware discovered in the same period in 2008," Dave Marcus, director of security research and communications at McAfee, said in a statement. "This tremendous growth is a signal of daunting times for users as malware infiltrates more and more of the platforms we trust."

The increase in the amount of malware equates to about 6,000 new samples daily. SC Magazine

Full Story :

<http://www.scmagazineus.com/Malware-pace-quickens-dramatically/article/140524/>

• Lawmakers: Electric utilities ignore cyber warnings

IDG News Service - The U.S. electrical grid remains vulnerable to cyber and electromagnetic pulse attacks despite years of warnings, several U.S. lawmakers said today.

The electric industry has pushed against federal cybersecurity standards and some utilities appear to be avoiding industry self-regulatory efforts by declining to designate their facilities or equipment as critical assets that need special protection, said U.S. Rep. Yvette Clarke, a New York Democrat and chairwoman of the House Homeland Security Committee's Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology.

"This effort seems to epitomize the head-in-the-sand mentality that seems to permeate broad sections of the electric industry," Clarke said. Computerworld

Full Story :

http://www.computerworld.com/s/article/9135753/Lawmakers_Electric_utilities_ignore_cyber_warnings?source=rss

New Vulnerabilities Tested in SecureScout

• 13709 MySQL dispatch_command function format string Vulnerabilities

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 COM_CREATE_DB or COM_DROP_DB request.

The issue has been fixed in version 5.0.84.

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

References:

- * BUGTRAQ: 20090708 MySQL <= 5.0.45 post auth format string vulnerability
<http://www.securityfocus.com/archive/1/archive/1/504799/100/0/threaded>
- * FULLDISC: 20090708 MySQL <= 5.0.45 post auth format string vulnerability
<http://archives.neohapsis.com/archives/fulldisclosure/2009-07/0058.html>
- * BID: 35609
<http://www.securityfocus.com/bid/35609>
- * OSVDB: 55734
<http://www.osvdb.org/55734>
- * SECTRAK: 1022533
<http://securitytracker.com/id?1022533>
- * SECUNIA: 35767
<http://secunia.com/advisories/35767>
- * VUPEN: ADV-2009-1857
<http://www.vupen.com/english/advisories/2009/1857>
- * XF: mysql-dispatchcommand-format-string(51614)
<http://xforce.iss.net/xforce/xfdb/51614>

CVE Reference:

CVE-2009-2446 (cve.mitre.org, nvd.nist.gov)

• 18447 Microsoft Office Publisher Pointer Dereference Vulnerability (MS09-030/969516) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Publisher opens, imports, and converts files created in versions older than Microsoft Office Publisher 2007. An attacker could exploit the vulnerability by creating a specially crafted Publisher file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

If a user were logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

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

References:

- * MS: MS09-030
<http://www.microsoft.com/technet/security/Bulletin/MS09-030.mspx>
- * BID: 35599
<http://www.securityfocus.com/bid/35599>
- * OSVDB: 55838
<http://osvdb.org/55838>
- * SECTRAK: 1022546
<http://www.securitytracker.com/id?1022546>
- * VUPEN: ADV-2009-1888
<http://www.vupen.com/english/advisories/2009/1888>

CVE Reference:

CVE-2009-0566 (cve.mitre.org, nvd.nist.gov)

• 18449 Wireshark PCNFSD dissector Denial of Service Vulnerability (CVE-2009-1829) (Remote File Checking)

Unspecified vulnerability in the PCNFSD dissector in Wireshark 0.8.20 through 1.0.7 allows remote attackers to cause a denial of service (crash) via crafted PCNFSD packets.

The vulnerability is reported in versions 0.8.20 up to and including 1.0.7.

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

References:

- * CONFIRM:
<http://wiki.rpath.com/wiki/Advisories:rPSA-2009-0095>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-03.html>
- * FEDORA: FEDORA-2009-5339

<https://www.redhat.com/archives/fedora-package-announce/2009-May/msg01167.html>

* FEDORA: FEDORA-2009-5382

<https://www.redhat.com/archives/fedora-package-announce/2009-May/msg01213.html>

* MANDRIVA: MDVSA-2009:125

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:125>

* REDHAT: RHSA-2009:1100

<http://www.redhat.com/support/errata/RHSA-2009-1100.html>

* BID: 35081

<http://www.securityfocus.com/bid/35081>

* OSVDB: 54629

<http://osvdb.org/54629>

* SECTRAK: 1022274

<http://www.securitytracker.com/id?1022274>

* SECUNIA: 35201

<http://secunia.com/advisories/35201>

* SECUNIA: 35248

<http://secunia.com/advisories/35248>

* SECUNIA: 35224

<http://secunia.com/advisories/35224>

* SECUNIA: 35464

<http://secunia.com/advisories/35464>

* VUPEN: ADV-2009-1408

<http://www.vupen.com/english/advisories/2009/1408>

* XF: wireshark-pcncfsd-dos(50686)

<http://xforce.iss.net/xforce/xfdb/50686>

CVE Reference:

CVE-2009-1829 (cve.mitre.org, nvd.nist.gov)

• 18450 Wireshark IPMI dissector buffer overflow Vulnerability (CVE-2009-2559) (Remote File Checking)

Buffer overflow in the IPMI dissector in Wireshark 1.2.0 allows remote attackers to cause a denial of service (crash) via unspecified vectors related to an array index error. NOTE: some of these details are obtained from third party information.

The vulnerability is reported in version 1.2.0.

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

References:

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2009-04.html>

* BID: 35748

<http://www.securityfocus.com/bid/35748>

* SECUNIA: 35884

<http://secunia.com/advisories/35884>

* VUPEN: ADV-2009-1970

<http://www.vupen.com/english/advisories/2009/1970>

CVE Reference:

CVE-2009-2559 (cve.mitre.org, nvd.nist.gov)

• 18451 Wireshark AFS dissector Denial of Service Vulnerability (CVE-2009-2562) (Remote File Checking)

Unspecified vulnerability in the AFS dissector in Wireshark 0.9.2 through 1.2.0 allows remote attackers to cause a denial of service (crash) via unknown vectors.

The vulnerability is reported in versions 0.9.2 up to and including 1.2.0.

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

References:

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2009-04.html>

* BID: 35748

<http://www.securityfocus.com/bid/35748>

* SECUNIA: 35884

<http://secunia.com/advisories/35884>

* VUPEN: ADV-2009-1970

<http://www.vupen.com/english/advisories/2009/1970>

CVE Reference:

CVE-2009-2562 (cve.mitre.org, nvd.nist.gov)

• 18452 Wireshark Infiniband dissector Denial of Service Vulnerability (CVE-2009-2563) (Remote File Checking)

Unspecified vulnerability in the Infiniband dissector in Wireshark 1.0.6 through 1.2.0, when running on unspecified platforms, allows remote attackers to cause a denial of service (crash) via unknown vectors.

The vulnerability is reported in versions 1.0.6 to 1.2.0.

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

References:

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2009-04.html>

* BID: 35748

<http://www.securityfocus.com/bid/35748>

* SECUNIA: 35884

<http://secunia.com/advisories/35884>

* VUPEN: ADV-2009-1970

<http://www.vupen.com/english/advisories/2009/1970>

CVE Reference:

CVE-2009-2563 (cve.mitre.org, nvd.nist.gov)

• 18453 Wireshark Bluetooth L2CAP dissector Denial of Service Vulnerability (CVE-2009-2560) (Remote File Checking)

Unspecified vulnerability in the Bluetooth L2CAP dissector in Wireshark 1.2.0, allows remote attackers to cause a denial of service (crash) via unknown vectors.

The vulnerability is reported in versions 1.2.0.

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

References:

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2009-04.html>

* BID: 35748

<http://www.securityfocus.com/bid/35748>

* SECUNIA: 35884

<http://secunia.com/advisories/35884>

* VUPEN: ADV-2009-1970

<http://www.vupen.com/english/advisories/2009/1970>

CVE Reference:

CVE-2009-2560 (cve.mitre.org, nvd.nist.gov)

• 18454 Wireshark RADIUS dissector Denial of Service Vulnerability (CVE-2009-2560) (Remote File Checking)

Unspecified vulnerability in the RADIUS dissector in Wireshark 1.2.0, allows remote attackers to cause a denial of service (crash) via unknown vectors.

The vulnerability is reported in versions 1.2.0.

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

References:

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2009-04.html>

* BID: 35748

<http://www.securityfocus.com/bid/35748>

* SECUNIA: 35884

<http://secunia.com/advisories/35884>

* VUPEN: ADV-2009-1970

<http://www.vupen.com/english/advisories/2009/1970>

CVE Reference:

CVE-2009-2560 (cve.mitre.org, nvd.nist.gov)

• 18455 Wireshark MIOP dissector Denial of Service Vulnerability (CVE-2009-2560) (Remote File Checking)

Unspecified vulnerability in the MIOP dissector in Wireshark 1.2.0, allows remote attackers to cause a denial of service (crash) via unknown vectors.

The vulnerability is reported in versions 1.2.0.

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

References:

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2009-04.html>

* BID: 35748

<http://www.securityfocus.com/bid/35748>

* SECUNIA: 35884

<http://secunia.com/advisories/35884>

* VUPEN: ADV-2009-1970

<http://www.vupen.com/english/advisories/2009/1970>

CVE Reference:

CVE-2009-2560 (cve.mitre.org, nvd.nist.gov)

• 18456 Wireshark sFlow dissector Denial of Service (CPU and memory consumption) Vulnerability (CVE-2009-2561) (Remote File Checking)

Unspecified vulnerability in the sFlow dissector in Wireshark 1.2.0 allows remote attackers to cause a denial of service (CPU and memory consumption) via unspecified vectors.

The vulnerability is reported in versions 1.2.0.

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

References:

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2009-04.html>

* BID: 35748

<http://www.securityfocus.com/bid/35748>

* SECUNIA: 35884

<http://secunia.com/advisories/35884>

* VUPEN: ADV-2009-1970

<http://www.vupen.com/english/advisories/2009/1970>

CVE Reference:

CVE-2009-2561 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-2576 Microsoft CVSS 2.0 Score = 5.0

Microsoft Internet Explorer 6.0.2900.2180 and earlier allows remote attackers to cause a denial of service (CPU and memory consumption) via a long Unicode string argument to the write method, a related issue to CVE-2009-2479.

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

References:

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/505122/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/505120/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/505092/100/0/threaded>

MISC: <http://websecurity.com.ua/3338/>

CVE Reference: [CVE-2009-2576](#)

• **CVE-2009-2536 Microsoft CVSS 2.0 Score = 4.3**

Microsoft Internet Explorer 5 through 8 allows remote attackers to cause a denial of service (memory consumption and application crash) via a large integer value for the length property of a Select object, a related issue to CVE-2009-1692.

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

References:

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/505006/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/504989/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/504988/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/504969/100/0/threaded>

MILWORM: <http://www.milw0rm.com/exploits/9160>

MISC: <http://www.g-sec.lu/one-bug-to-rule-them-all.html>

CVE Reference: [CVE-2009-2536](#)

• **CVE-2009-2570 Symantec CVSS 2.0 Score = 10.0**

Stack-based buffer overflow in the Symantec.FaxViewerControl.1 ActiveX control in WinFax\DCCFAXVW.DLL in Symantec WinFax Pro 10.03 allows remote attackers to execute arbitrary code via a long argument to the AppendFax method.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/1221>

SECTRAK: <http://www.securitytracker.com/id?1022147>

BID: <http://www.securityfocus.com/bid/34766>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/503163/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/503086/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/503074/100/0/threaded>

SECUNIA: <http://secunia.com/advisories/34925>

MISC: http://retrogod.altervista.org/9sq_symantec_win_fuck_pro.html

OSVDB: <http://osvdb.org/54137>

CVE Reference: [CVE-2009-2570](#)

• **CVE-2009-2543 IBM CVSS 2.0 Score = 10.0**

Multiple unspecified vulnerabilities in the IBM Proventia engine 4.9.0.0.44 20081231, as used in IBM Proventia Network Mail Security System, Network Mail Security System Virtual Appliance, Desktop Endpoint Security, Network Multi-Function Security (MFS), and possibly other products, allow remote attackers to bypass detection of malware via a modified (1) ZIP or (2) CAB archive, a related issue to CVE-2009-1240.

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

References:

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/504995/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/504992/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/504987/100/0/threaded>

MISC: http://iss.custhelp.com/cgi-bin/iss.cfg/php/enduser/std_adp.php?p_faqid=5417

CVE Reference: [CVE-2009-2543](#)

• **CVE-2009-2462 Mozilla CVSS 2.0 Score = 10.0**

The browser engine in Mozilla Firefox before 3.0.12 and Thunderbird allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) the frame chain and synchronous events, (2) a SetMayHaveFrame assertion and nsCSSFrameConstructor::CreateFloatingLetterFrame, (3) nsCSSFrameConstructor::ConstructFrame, (4) the child list and initial reflow, (5) GetLastSpecialSibling, (6) nsFrameManager::GetPrimaryFrameFor and MathML, (7) nsFrame::GetBoxAscent, (8) nsCSSFrameConstructor::AdjustParentFrame, (9) nsDOMOfflineResourceList, and (10) nsContentUtils::ComparePosition.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/1972>

BID: <http://www.securityfocus.com/bid/35758>

CONFIRM: <http://www.mozilla.org/security/announce/2009/mfsa2009-34.html>

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=491134

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=472950

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=472668

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=468211

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=466763

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=463350

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=461861

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=445177

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=442227

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=413085

SECUNIA: <http://secunia.com/advisories/35947>

SECUNIA: <http://secunia.com/advisories/35944>

SECUNIA: <http://secunia.com/advisories/35943>

SECUNIA: <http://secunia.com/advisories/35914>

REDHAT: <http://rhn.redhat.com/errata/RHSA-2009-1163.html>

REDHAT: <http://rhn.redhat.com/errata/RHSA-2009-1162.html>

CVE Reference: [CVE-2009-2462](#)

• **CVE-2009-2463 Mozilla CVSS 2.0 Score = 10.0**

Integer overflow in a base64 decoding function in Mozilla Firefox before 3.0.12 and Thunderbird allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/1972>

BID: <http://www.securityfocus.com/bid/35758>

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=492779

CONFIRM: <http://www.mozilla.org/security/announce/2009/mfsa2009-34.html>

SECUNIA: <http://secunia.com/advisories/35947>

SECUNIA: <http://secunia.com/advisories/35944>

SECUNIA: <http://secunia.com/advisories/35943>

SECUNIA: <http://secunia.com/advisories/35914>

REDHAT: <http://rhn.redhat.com/errata/RHSA-2009-1163.html>

REDHAT: <http://rhn.redhat.com/errata/RHSA-2009-1162.html>

CVE Reference: [CVE-2009-2463](#)

• **CVE-2009-2464 Mozilla CVSS 2.0 Score = 10.0**

The nsXULTemplateQueryProcessorRDF::CheckIsSeparator function in Mozilla Firefox before 3.0.12, SeaMonkey 2.0a1pre, and Thunderbird allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to loading multiple RDF files in a XUL tree element.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/1972>

BID: <http://www.securityfocus.com/bid/35758>

CONFIRM: <http://www.mozilla.org/security/announce/2009/mfsa2009-34.html>

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=441785

SECUNIA: <http://secunia.com/advisories/35944>

SECUNIA: <http://secunia.com/advisories/35943>

SECUNIA: <http://secunia.com/advisories/35914>

REDHAT: <http://rhn.redhat.com/errata/RHSA-2009-1162.html>

CVE Reference: [CVE-2009-2464](#)

• **CVE-2009-2465 Mozilla CVSS 2.0 Score = 10.0**

Mozilla Firefox before 3.0.12 and Thunderbird allow remote attackers to cause a denial of service (memory corruption and application crash) or execute arbitrary code via vectors involving double frame construction, related to (1) nsHTMLContentSink.cpp, (2) nsXMLContentSink.cpp, and (3) nsPresShell.cpp, and the nsSubDocumentFrame::Reflow function.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/1972>

BID: <http://www.securityfocus.com/bid/35758>

CONFIRM: <http://www.mozilla.org/security/announce/2009/mfsa2009-34.html>

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=489050

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=482578

SECUNIA: <http://secunia.com/advisories/35944>

SECUNIA: <http://secunia.com/advisories/35943>

SECUNIA: <http://secunia.com/advisories/35914>

REDHAT: <http://rhn.redhat.com/errata/RHSA-2009-1162.html>

CVE Reference: [CVE-2009-2465](#)

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

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

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