

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

Cyber security one task of many for new president Obama. Compliance deadlines have been set. Security top priority for IT organizations. ISP's facing threats.

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

• Cybersecurity advice for President-elect Obama to be previewed at SC World Congress

Among the challenges President-elect Barack Obama will inherit when he is inaugurated on Jan. 20 is a national cyberinfrastructure under almost constant attack. But he and his administration will be receiving a good deal of assistance in that regard from the Commission on Cyber Security for the 44th Presidency, set up last October by the Center for Strategic and International Studies (CSIS).

The CSIS, a bipartisan, nonprofit organization headquartered in Washington, D.C., provides strategic insights and policy solutions to decision-makers in government, international institutions and the private sector. Its Commission on Cyber Security for the 44th Presidency will offer recommendations to the 44th president on a comprehensive strategy for organizing and prioritizing efforts to secure America's computer networks and critical infrastructure.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Cybersecurity-advice-for-President-elect-Obama-to-be-previewed-at-SC-World-Congr>

- **Visa sets PCI compliance deadlines for rest of world**

The largest merchants operating overseas will have less than two years to secure credit card transactions, Visa announced on Monday.

Level-one retailers -- those processing more than six million Visa transactions per year -- must prove adherence to the Payment Card Industry Data Security Standard (PCI DSS) by Sept. 30, 2010, Visa said in a news release. After that date, Visa may begin issuing fines to acquiring banks, which typically pass the penalties down to the merchants.

Visa also announced that as of Sept. 30, 2009, level-one and level-two merchants -- which process between one and six million Visa transactions -- cannot retain any data encoded on the magnetic stripe on the back of the card, such as PINs or security codes.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Visa-sets-PCI-compliance-deadlines-for-rest-of-world/article/120734/>

- **Security, virtualization lead 2009 tech plans**

November 11, 2008 (Network World) IT organizations consider security, server virtualization and business-related technologies a top priority for 2009, according to research released by The Society for Information Management.

Jerry Luftman, SIM vice president for academic affairs and distinguished professor and associate dean at the Stevens Institute, said the highest ranking technologies reflect a few key issues on IT leaders' minds.

To start, security via antivirus protection reflects IT's ongoing balancing act between enabling services while also protecting environments. IT organizations are also tasked with combating more varied threats than in the past.(Compare Secure Web Gateway products.) Kenneth Washington, chief privacy officer and vice president at Lockheed Martin, explained to attendees how people are hyperconnected via multiple devices today, which poses a challenge to security and privacy leaders tasked with securing networks.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9119842&source=rss_topic1

- **Study: Internet service providers facing more, larger threats**

Internet service providers (ISPs) are facing more security threats, while attacks are becoming larger and more sophisticated.

That finding is from Arbor Networks' Worldwide Infrastructure Security Report, released Tuesday. The report compiles survey responses from 66 lead security engineers from North America, South America, Europe and Asia. They were asked questions relating to internet security threats and engineering challenges occurring between August 2007 and July 2008.

In last year's report, the largest sustained DDoS attack was 24 gigabits. In 2001, the largest was only 400 megabits per second. This year's largest attack represents a 100-fold increase over 2001, the report states.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Study-Internet-service-providers-facing-more-larger-threats/article/120828/>

New Vulnerabilities Tested in SecureScout

- **18186 OpenSSL ASN.1 Large Recursion Remote Denial Of Service Vulnerability**

OpenSSL 0.9.6k allows remote attackers to cause a denial of service (crash via large recursion) via malformed ASN.1 sequences.

The issue has been fixed in version 0.9.6l.

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

References:

* BUGTRAQ: 20031104 [OpenSSL Advisory] Denial of Service in ASN.1 parsing
<http://marc.theaimsgroup.com/?l=bugtraq&m=106796246511667&w=2>

* CONFIRM:
http://www.openssl.org/news/secadv_20031104.txt
* CISCO: 20030930 SSL Implementation Vulnerabilities
<http://www.cisco.com/warp/public/707/cisco-sa-20030930-ssl.shtml>
* FEDORA: FEDORA-2005-1042
<http://www.redhat.com/archives/fedora-announce-list/2005-October/msg00087.html>
* NETBSD: NetBSD-SA2004-003
<ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-003.txt.asc>
* REDHAT: RHSA-2004:119
<http://rhn.redhat.com/errata/RHSA-2004-119.html>
* SGI: 20040304-01-U
<ftp://patches.sgi.com/support/free/security/advisories/20040304-01-U.asc>
* BUGTRAQ: 20040508 [FLSA-2004:1395] Updated OpenSSL resolves security vulnerability
<http://marc.theaimsgroup.com/?l=bugtraq&m=108403850228012&w=2>
* CERT-VN: VU#412478
<http://www.kb.cert.org/vuls/id/412478>
* BID: 8970
<http://www.securityfocus.com/bid/8970>
* SECUNIA: 17381
<http://secunia.com/advisories/17381>

CVE Reference:

CVE-2003-0851 (cve.mitre.org, nvd.nist.gov)

• 18188 Apache HTTP Server mod_proxy crash Vulnerability

The date handling code in modules/proxy/proxy_util.c (mod_proxy) in Apache, when using a threaded MPM, allows remote origin servers to cause a denial of service (caching forward proxy process crash) via crafted date headers that trigger a buffer over-read.

The issue has been fixed in version 2.2.6.

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

References:

* MISC: The Apache HTTP Server Project
<http://httpd.apache.org/>
* MLIST: [apache-cvs] 20070801 svn commit: r561616 - in /httpd/httpd/trunk: CHANGES
<http://marc.info/?l=apache-cvs&m=118592992309395&w=2>
* MLIST: [apache-httpd-dev] 20070801 Re: svn commit: r561616 - in /httpd/httpd/trunk: CHANGES
modules/proxy/proxy_util.c
<http://marc.info/?l=apache-httpd-dev&m=118595556504202&w=2>
* MLIST: [apache-httpd-dev] 20070801 Re: svn commit: r561616 - in /httpd/httpd/trunk: CHANGES
modules/proxy/proxy_util.c
<http://marc.info/?l=apache-httpd-dev&m=118595953217856&w=2>
* CONFIRM:
http://httpd.apache.org/security/vulnerabilities_20.html
* CONFIRM:
http://httpd.apache.org/security/vulnerabilities_22.html
* CONFIRM:
<https://issues.rpath.com/browse/RPL-1710>
* CONFIRM:
http://bugs.gentoo.org/show_bug.cgi?id=186219
* CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2007-500.htm>
* CONFIRM:
<http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg27007951>
* CONFIRM:
<http://www.fujitsu.com/global/support/software/security/products-f/interstage-200802e.html>
* CONFIRM:
<http://docs.info.apple.com/article.html?artnum=307562>
* AIXAPAR: PK50469
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK50469>
* AIXAPAR: PK52702
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK52702>
* APPLE: APPLE-SA-2008-03-18
<http://lists.apple.com/archives/security-announce/2008/Mar/msg00001.html>
* APPLE: APPLE-SA-2008-05-28
<http://lists.apple.com/archives/security-announce/2008/May/msg00001.html>

* FEDORA: FEDORA-2007-2214
<http://www.redhat.com/archives/fedora-package-announce/2007-September/msg00320.html>

* FEDORA: FEDORA-2007-707
<https://www.redhat.com/archives/fedora-package-announce/2007-September/msg00353.html>

* GENTOO: GLSA-200711-06
<http://security.gentoo.org/glsa/glsa-200711-06.xml>

* HP: HPSBUX02273
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01182588>

* MANDRIVA: MDKSA-2007:235
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:235>

* REDHAT: RHSA-2007:0911
<http://www.redhat.com/support/errata/RHSA-2007-0911.html>

* REDHAT: RHSA-2007:0746
<http://www.redhat.com/support/errata/RHSA-2007-0746.html>

* REDHAT: RHSA-2007:0747
<http://www.redhat.com/support/errata/RHSA-2007-0747.html>

* REDHAT: RHSA-2008:0005
<http://www.redhat.com/support/errata/RHSA-2008-0005.html>

* SLACKWARE: SSA:2008-045-02
<http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.595748>

* SUSE: SUSE-SA:2007:061
http://www.novell.com/linux/security/advisories/2007_61_apache2.html

* UBUNTU: USN-575-1
<http://www.ubuntu.com/usn/usn-575-1>

* CERT: TA08-150A
<http://www.us-cert.gov/cas/techalerts/TA08-150A.html>

* BID: 25489
<http://www.securityfocus.com/bid/25489>

* FRSIRT: ADV-2007-3020
<http://www.frsirt.com/english/advisories/2007/3020>

* FRSIRT: ADV-2007-3095
<http://www.frsirt.com/english/advisories/2007/3095>

* FRSIRT: ADV-2007-3283
<http://www.frsirt.com/english/advisories/2007/3283>

* FRSIRT: ADV-2007-3494
<http://www.frsirt.com/english/advisories/2007/3494>

* FRSIRT: ADV-2007-3955
<http://www.frsirt.com/english/advisories/2007/3955>

* FRSIRT: ADV-2008-0924
<http://www.frsirt.com/english/advisories/2008/0924/references>

* FRSIRT: ADV-2008-1697
<http://www.frsirt.com/english/advisories/2008/1697>

* SECTRAK: 1018633
<http://www.securitytracker.com/id?1018633>

* SECUNIA: 26636
<http://secunia.com/advisories/26636>

* SECUNIA: 26722
<http://secunia.com/advisories/26722>

* SECUNIA: 26790
<http://secunia.com/advisories/26790>

* SECUNIA: 26842
<http://secunia.com/advisories/26842>

* SECUNIA: 26952
<http://secunia.com/advisories/26952>

* SECUNIA: 26993
<http://secunia.com/advisories/26993>

* SECUNIA: 27209
<http://secunia.com/advisories/27209>

* SECUNIA: 27563
<http://secunia.com/advisories/27563>

* SECUNIA: 27593
<http://secunia.com/advisories/27593>

* SECUNIA: 27732
<http://secunia.com/advisories/27732>

* SECUNIA: 27882
<http://secunia.com/advisories/27882>

* SECUNIA: 27971
<http://secunia.com/advisories/27971>

* SECUNIA: 28467

<http://secunia.com/advisories/28467>

* SECUNIA: 28749

<http://secunia.com/advisories/28749>

* SECUNIA: 28606

<http://secunia.com/advisories/28606>

* SECUNIA: 28922

<http://secunia.com/advisories/28922>

* SECUNIA: 29420

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

* SECUNIA: 30430

<http://secunia.com/advisories/30430>

CVE Reference:

CVE-2007-3847 (cve.mitre.org, nvd.nist.gov)

• 18189 Apache HTTP Server mod_status cross-site scripting Vulnerability

Cross-site scripting (XSS) vulnerability in mod_status.c in the mod_status module in Apache HTTP Server (httpd), when ExtendedStatus is enabled and a public server-status page is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors involving charsets with browsers that perform "charset detection" when the content-type is not specified.

The issue has been fixed in version 2.2.6.

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

References:

* MISC: The Apache HTTP Server Project

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

* MISC:

http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=245112

* CONFIRM:

<http://svn.apache.org/viewvc?view=rev&revision=549159>

* CONFIRM:

<https://issues.rpath.com/browse/RPL-1500>

* CONFIRM:

http://httpd.apache.org/security/vulnerabilities_13.html

* CONFIRM:

http://httpd.apache.org/security/vulnerabilities_20.html

* CONFIRM:

http://httpd.apache.org/security/vulnerabilities_22.html

* CONFIRM:

<http://support.avaya.com/elmodocs2/security/ASA-2007-353.htm>

* CONFIRM:

http://bugs.gentoo.org/show_bug.cgi?id=186219

* CONFIRM:

<http://www.fujitsu.com/global/support/software/security/products-f/interstage-200802e.html>

* AIXAPAR: PK49295

<http://www-1.ibm.com/support/search.wss?rs=0&q=PK49295&apar=only>

* AIXAPAR: PK52702

<http://www-1.ibm.com/support/docview.wss?uid=swg1PK52702>

* FEDORA: FEDORA-2007-2214

<http://www.redhat.com/archives/fedora-package-announce/2007-September/msg00320.html>

* GENTOO: GLSA-200711-06

<http://security.gentoo.org/glsa/glsa-200711-06.xml>

* HP: HPSBUX02262

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01178795>

* MANDRIVA: MDKSA-2007:140

<http://www.mandriva.com/security/advisories?name=MDKSA-2007:140>

* MANDRIVA: MDKSA-2007:141

<http://www.mandriva.com/security/advisories?name=MDKSA-2007:141>

* MANDRIVA: MDKSA-2007:142

<http://www.mandriva.com/security/advisories?name=MDKSA-2007:142>

* REDHAT: RHSA-2007:0532

<http://www.redhat.com/support/errata/RHSA-2007-0532.html>

* REDHAT: RHSA-2007:0534

<http://rhn.redhat.com/errata/RHSA-2007-0534.html>

* REDHAT: RHSA-2007:0556

<http://rhn.redhat.com/errata/RHSA-2007-0556.html>

* REDHAT: RHSA-2007:0533
<https://rhn.redhat.com/errata/RHSA-2007-0533.html>

* REDHAT: RHSA-2007:0557
<http://www.redhat.com/support/errata/RHSA-2007-0557.html>

* REDHAT: RHSA-2008:0261
<http://www.redhat.com/support/errata/RHSA-2008-0261.html>

* SUNALERT: 103179
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-103179-1>

* SUNALERT: 200032
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-200032-1>

* UBUNTU: USN-499-1
<http://www.ubuntu.com/usn/usn-499-1>

* BID: 24645
<http://www.securityfocus.com/bid/24645>

* FRSIRT: ADV-2007-2727
<http://www.frsirt.com/english/advisories/2007/2727>

* FRSIRT: ADV-2007-3283
<http://www.frsirt.com/english/advisories/2007/3283>

* FRSIRT: ADV-2007-3386
<http://www.frsirt.com/english/advisories/2007/3386>

* FRSIRT: ADV-2007-4305
<http://www.frsirt.com/english/advisories/2007/4305>

* SECTRAK: 1018302
<http://www.securitytracker.com/id?1018302>

* SECUNIA: 25827
<http://secunia.com/advisories/25827>

* SECUNIA: 25830
<http://secunia.com/advisories/25830>

* SECUNIA: 25873
<http://secunia.com/advisories/25873>

* SECUNIA: 25920
<http://secunia.com/advisories/25920>

* SECUNIA: 26273
<http://secunia.com/advisories/26273>

* SECUNIA: 26443
<http://secunia.com/advisories/26443>

* SECUNIA: 26458
<http://secunia.com/advisories/26458>

* SECUNIA: 26508
<http://secunia.com/advisories/26508>

* SECUNIA: 26822
<http://secunia.com/advisories/26822>

* SECUNIA: 26842
<http://secunia.com/advisories/26842>

* SECUNIA: 26993
<http://secunia.com/advisories/26993>

* SECUNIA: 27037
<http://secunia.com/advisories/27037>

* SECUNIA: 27563
<http://secunia.com/advisories/27563>

* SECUNIA: 27732
<http://secunia.com/advisories/27732>

* SECUNIA: 28212
<http://secunia.com/advisories/28212>

* SECUNIA: 28224
<http://secunia.com/advisories/28224>

* SECUNIA: 28606
<http://secunia.com/advisories/28606>

* XF: apache-modstatus-xss(35097)
<http://xforce.iss.net/xforce/xfdb/35097>

CVE Reference:

CVE-2006-5752 (cve.mitre.org, nvd.nist.gov)

• 18190 Apache HTTP Server mod_cache information leak Vulnerability

The recall_headers function in mod_mem_cache in Apache 2.2.4 does not properly copy all levels of header data, which can cause Apache to return HTTP headers containing previously used data, which could be used by remote attackers to obtain potentially sensitive information.

The issue has been fixed in version 2.2.6.

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

References:

- * MISC: The Apache HTTP Server Project
<http://httpd.apache.org/>
- * CONFIRM:
http://issues.apache.org/bugzilla/show_bug.cgi?id=41551
- * CONFIRM:
http://people.apache.org/~covener/2.2.x-mod_memcache-poolmgmt.diff
- * CONFIRM:
http://httpd.apache.org/security/vulnerabilities_22.html
- * CONFIRM:
http://bugs.gentoo.org/show_bug.cgi?id=186219
- * FEDORA: FEDORA-2007-2214
<http://www.redhat.com/archives/fedora-package-announce/2007-September/msg00320.html>
- * GENTOO: GLSA-200711-06
<http://security.gentoo.org/glsa/glsa-200711-06.xml>
- * MANDRIVA: MDKSA-2007:127
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:127>
- * BID: 24553
<http://www.securityfocus.com/bid/24553>
- * FRSIRT: ADV-2007-2231
<http://www.frsirt.com/english/advisories/2007/2231>
- * FRSIRT: ADV-2007-2727
<http://www.frsirt.com/english/advisories/2007/2727>
- * SECUNIA: 26273
<http://secunia.com/advisories/26273>
- * SECUNIA: 26842
<http://secunia.com/advisories/26842>
- * SECUNIA: 27563
<http://secunia.com/advisories/27563>

CVE Reference:

CVE-2007-1862 (cve.mitre.org, nvd.nist.gov)

• 18191 Apache HTTP Server mod_cache proxy DoS Vulnerability

cache_util.c in the mod_cache module in Apache HTTP Server (httpd), when caching is enabled and a threaded Multi-Processing Module (MPM) is used, allows remote attackers to cause a denial of service (child processing handler crash) via a request with the (1) s-maxage, (2) max-age, (3) min-fresh, or (4) max-stale Cache-Control headers without a value.

The issue has been fixed in version 2.0.61, and 2.2.6.

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

References:

- * MISC: The Apache HTTP Server Project
<http://httpd.apache.org/>
- * MISC:
http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=244658
- * CONFIRM:
<http://svn.apache.org/viewvc?view=rev&revision=535617>
- * CONFIRM:
<https://issues.rpath.com/browse/RPL-1500>
- * CONFIRM:
http://httpd.apache.org/security/vulnerabilities_20.html
- * CONFIRM:
http://httpd.apache.org/security/vulnerabilities_22.html
- * CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2007-353.htm>
- * CONFIRM:
http://bugs.gentoo.org/show_bug.cgi?id=186219
- * CONFIRM:
<http://www.fujitsu.com/global/support/software/security/products-f/interstage-200802e.html>
- * AIXAPAR: PK49355
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK49355>

* AIXAPAR: PK52702
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK52702>

* APPLE: APPLE-SA-2008-05-28
<http://lists.apple.com/archives/security-announce/2008//May/msg00001.html>

* FEDORA: FEDORA-2007-2214
<http://www.redhat.com/archives/fedora-package-announce/2007-September/msg00320.html>

* GENTOO: GLSA-200711-06
<http://security.gentoo.org/glsa/glsa-200711-06.xml>

* HP: HPSBUX02262
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01178795>

* MANDRIVA: MDKSA-2007:140
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:140>

* MANDRIVA: MDKSA-2007:141
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:141>

* REDHAT: RHSA-2007:0534
<http://rhn.redhat.com/errata/RHSA-2007-0534.html>

* REDHAT: RHSA-2007:0556
<http://rhn.redhat.com/errata/RHSA-2007-0556.html>

* REDHAT: RHSA-2007:0533
<https://rhn.redhat.com/errata/RHSA-2007-0533.html>

* REDHAT: RHSA-2007:0557
<http://www.redhat.com/support/errata/RHSA-2007-0557.html>

* SUSE: SUSE-SA:2007:061
http://www.novell.com/linux/security/advisories/2007_61_apache2.html

* UBUNTU: USN-499-1
<http://www.ubuntu.com/usn/usn-499-1>

* CERT: TA08-150A
<http://www.us-cert.gov/cas/techalerts/TA08-150A.html>

* BID: 24649
<http://www.securityfocus.com/bid/24649>

* FRSIRT: ADV-2007-2727
<http://www.frsirt.com/english/advisories/2007/2727>

* FRSIRT: ADV-2007-3283
<http://www.frsirt.com/english/advisories/2007/3283>

* FRSIRT: ADV-2007-3386
<http://www.frsirt.com/english/advisories/2007/3386>

* FRSIRT: ADV-2008-1697
<http://www.frsirt.com/english/advisories/2008/1697>

* SECTRAK: 1018303
<http://www.securitytracker.com/id?1018303>

* SECUNIA: 25830
<http://secunia.com/advisories/25830>

* SECUNIA: 25873
<http://secunia.com/advisories/25873>

* SECUNIA: 25920
<http://secunia.com/advisories/25920>

* SECUNIA: 26273
<http://secunia.com/advisories/26273>

* SECUNIA: 26443
<http://secunia.com/advisories/26443>

* SECUNIA: 26508
<http://secunia.com/advisories/26508>

* SECUNIA: 26822
<http://secunia.com/advisories/26822>

* SECUNIA: 26842
<http://secunia.com/advisories/26842>

* SECUNIA: 26993
<http://secunia.com/advisories/26993>

* SECUNIA: 27037
<http://secunia.com/advisories/27037>

* SECUNIA: 27563
<http://secunia.com/advisories/27563>

* SECUNIA: 27732
<http://secunia.com/advisories/27732>

* SECUNIA: 28606
<http://secunia.com/advisories/28606>

* SECUNIA: 30430
<http://secunia.com/advisories/30430>

CVE Reference:

CVE-2007-1863 (cve.mitre.org, nvd.nist.gov)

• 18192 Apache HTTP Server mod_imap Referer Cross-Site Scripting Vulnerability

Cross-site scripting (XSS) vulnerability in the mod_imap module of Apache httpd before 1.3.35-dev and Apache httpd 2.0.x before 2.0.56-dev allows remote attackers to inject arbitrary web script or HTML via the Referer when using image maps.

The issue has been fixed in version 1.3.35, 2.0.58, 2.2.2.

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

References:

- * MISC: The Apache HTTP Server Project
<http://httpd.apache.org/>
- * CONFIRM:
http://issues.apache.org/bugzilla/show_bug.cgi?id=37874
- * CONFIRM:
<http://docs.info.apple.com/article.html?artnum=307562>
- * AIXAPAR: PK16139
<http://www-1.ibm.com/support/search.wss?rs=0&q=PK16139&apar=only>
- * AIXAPAR: PK25355
<http://www-1.ibm.com/support/search.wss?rs=0&q=PK25355&apar=only>
- * APPLE: APPLE-SA-2008-03-18
<http://lists.apple.com/archives/security-announce/2008/Mar/msg00001.html>
- * APPLE: APPLE-SA-2008-05-28
<http://lists.apple.com/archives/security-announce/2008/May/msg00001.html>
- * DEBIAN: DSA-1167
<http://www.debian.org/security/2006/dsa-1167>
- * FEDORA: FEDORA-2006-052
<http://www.redhat.com/archives/fedora-announce-list/2006-January/msg00060.html>
- * FEDORA: FLSA-2006:175406
<http://www.securityfocus.com/archive/1/archive/1/425399/100/0/threaded>
- * GENTOO: GLSA-200602-03
<http://www.gentoo.org/security/en/glsa/glsa-200602-03.xml>
- * HP: HPSBUX02145
<http://www.securityfocus.com/archive/1/archive/1/445206/100/0/threaded>
- * HP: HPSBUX02164
<http://www.securityfocus.com/archive/1/archive/1/450321/100/0/threaded>
- * HP: HPSBUX02172
<http://www.securityfocus.com/archive/1/archive/1/450315/100/0/threaded>
- * HP: HPSBMA02328
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01428449>
- * MANDRIVA: MDKSA-2006:007
<http://www.new.mandriva.com/security/advisories?name=MDKSA-2006:007>
- * OPENPKG: OpenPKG-SA-2005.029
<http://www.openpkg.org/security/OpenPKG-SA-2005.029-apache.txt>
- * REDHAT: RHSA-2006:0159
<http://rhn.redhat.com/errata/RHSA-2006-0159.html>
- * REDHAT: RHSA-2006:0158
<http://www.redhat.com/support/errata/RHSA-2006-0158.html>
- * REDHAT: RHSA-2006:0692
<http://rhn.redhat.com/errata/RHSA-2006-0692.html>
- * SGI: 20060101-01-U
<ftp://patches.sgi.com/support/free/security/advisories/20060101-01-U>
- * SLACKWARE: SSA:2006-129-01
<http://slackware.com/security/viewer.php?l=slackware-security&y=2006&m=slackware-security.685483>
- * SLACKWARE: SSA:2006-130-01
<http://slackware.com/security/viewer.php?l=slackware-security&y=2006&m=slackware-security.470158>
- * SUNALERT: 102662
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102662-1>
- * SUNALERT: 102663
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102663-1>
- * SUSE: SUSE-SA:2006:043
http://www.novell.com/linux/security/advisories/2006_43_apache.html
- * SUSE: SUSE-SR:2007:011
<http://lists.suse.com/archive/suse-security-announce/2007-May/0005.html>
- * TRUSTIX: TSLSA-2005-0074
<http://www.trustix.org/errata/2005/0074/>
- * UBUNTU: USN-241-1

<http://www.ubuntulinux.org/usn/usn-241-1>
* CERT: TA08-150A
<http://www.us-cert.gov/cas/techalerts/TA08-150A.html>
* BID: 15834
<http://www.securityfocus.com/bid/15834>
* FRSIRT: ADV-2005-2870
<http://www.frsirt.com/english/advisories/2005/2870>
* FRSIRT: ADV-2006-2423
<http://www.frsirt.com/english/advisories/2006/2423>
* FRSIRT: ADV-2006-3995
<http://www.frsirt.com/english/advisories/2006/3995>
* FRSIRT: ADV-2006-4015
<http://www.frsirt.com/english/advisories/2006/4015>
* FRSIRT: ADV-2006-4300
<http://www.frsirt.com/english/advisories/2006/4300>
* FRSIRT: ADV-2006-4868
<http://www.frsirt.com/english/advisories/2006/4868>
* FRSIRT: ADV-2008-0924
<http://www.frsirt.com/english/advisories/2008/0924/references>
* FRSIRT: ADV-2008-1246
<http://www.frsirt.com/english/advisories/2008/1246/references>
* FRSIRT: ADV-2008-1697
<http://www.frsirt.com/english/advisories/2008/1697>
* SECTRAK: 1015344
<http://securitytracker.com/id?1015344>
* SECUNIA: 18008
<http://secunia.com/advisories/18008>
* SECUNIA: 18333
<http://secunia.com/advisories/18333>
* SECUNIA: 18339
<http://secunia.com/advisories/18339>
* SECUNIA: 18340
<http://secunia.com/advisories/18340>
* SECUNIA: 18429
<http://secunia.com/advisories/18429>
* SECUNIA: 18585
<http://secunia.com/advisories/18585>
* SECUNIA: 18517
<http://secunia.com/advisories/18517>
* SECUNIA: 18743
<http://secunia.com/advisories/18743>
* SECUNIA: 17319
<http://secunia.com/advisories/17319>
* SECUNIA: 18526
<http://secunia.com/advisories/18526>
* SECUNIA: 19012
<http://secunia.com/advisories/19012>
* SECUNIA: 20670
<http://secunia.com/advisories/20670>
* SECUNIA: 21744
<http://secunia.com/advisories/21744>
* SECUNIA: 22140
<http://secunia.com/advisories/22140>
* SECUNIA: 22368
<http://secunia.com/advisories/22368>
* SECUNIA: 22388
<http://secunia.com/advisories/22388>
* SECUNIA: 22669
<http://secunia.com/advisories/22669>
* SECUNIA: 23260
<http://secunia.com/advisories/23260>
* SECUNIA: 20046
<http://secunia.com/advisories/20046>
* SECUNIA: 25239
<http://secunia.com/advisories/25239>
* SECUNIA: 29420
<http://secunia.com/advisories/29420>
* SECUNIA: 29849
<http://secunia.com/advisories/29849>

* SECUNIA: 30430
<http://secunia.com/advisories/30430>

CVE Reference:

CVE-2005-3352 (cve.mitre.org, nvd.nist.gov)

• 18210 MSXML Memory Corruption Vulnerability (MS08-069/955218) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft XML Core Services parses XML content. The vulnerability could allow remote code execution if a user browses a Web site that contains specially crafted content or opens specially crafted HTML e-mail. 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 impacted than users who operate with administrative user rights.

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

References:

- * BUGTRAQ: 20070104 Concurrency strikes MSIE (potentially exploitable msxml3 flaws)
<http://www.securityfocus.com/archive/1/archive/1/455965/100/0/threaded>
- * BUGTRAQ: 20070104 RE: [Full-disclosure] Concurrency strikes MSIE (potentially exploitablemsxml3 flaws)
<http://www.securityfocus.com/archive/1/archive/1/455986/100/0/threaded>
- * BUGTRAQ: 20070104 Re: RE: [Full-disclosure] Concurrency strikes MSIE (potentially exploitablemsxml3 flaws)
<http://www.securityfocus.com/archive/1/archive/1/456343/100/0/threaded>
- * FULLDISC: 20070104 Concurrency strikes MSIE (potentially exploitable msxml3 flaws)
<http://seclists.org/fulldisclosure/2007/Jan/0110.html>
- * MISC:
<http://isc.sans.org/diary.php?storyid=2004>
- * BID: 21872
<http://www.securityfocus.com/bid/21872>
- * SECUNIA: 23655
<http://secunia.com/advisories/23655>

CVE Reference:

CVE-2007-0099 (cve.mitre.org, nvd.nist.gov)

• 18211 MSXML DTD Cross-Domain Scripting Vulnerability (MS08-069/955218) (Remote File Checking)

An information disclosure vulnerability exists in the way that Microsoft XML Core Services handles error checks for external document type definitions (DTDs). The vulnerability could allow information disclosure if a user browses a Web site that contains specially crafted content or opens specially crafted HTML e-mail. An attacker who successfully exploited this vulnerability could read data from a Web page in another domain in Internet Explorer. In all cases, however, an attacker would have no way to force users to visit these Web sites.

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

References:

- * MS: MS08-069
<http://www.microsoft.com/technet/security/bulletin/ms08-069.msp>

CVE Reference:

CVE-2008-4029 (cve.mitre.org, nvd.nist.gov)

• 18212 MSXML Header Request Vulnerability (MS08-069/955218) (Remote File Checking)

An information disclosure vulnerability exists in the way that Microsoft XML Core Services handles transfer-encoding headers. The vulnerability could allow information disclosure if a user browses a Web site that contains specially crafted content or opens specially crafted HTML e-mail. An attacker who successfully exploited this vulnerability could read data from a Web page in another domain in Internet Explorer. In all cases, however, an attacker would have no way to force users to visit these Web sites.

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

References:

- * MS: MS08-069
<http://www.microsoft.com/technet/security/bulletin/ms08-069.msp>

CVE Reference:

CVE-2008-4033 (cve.mitre.org, nvd.nist.gov)

- **18213 SMB Credential Reflection Vulnerability (MS08-068/957097) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol handles NTLM credentials when a user connects to an attacker's SMB server. This vulnerability allows an attacker to replay the user's credentials back to them and execute code in the context of the logged-on user. If a user is 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 impacted than users who operate with administrative user rights.

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

References:

* MS: MS08-068

<http://www.microsoft.com/technet/security/bulletin/ms08-068.msp>

CVE Reference:

CVE-2008-4037 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2008-4037 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Windows 2000 Gold through SP4, XP Gold through SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote SMB servers to execute arbitrary code on a client machine by replaying the NTLM credentials of a client user, as demonstrated by backrush, aka "SMB Credential Reflection Vulnerability."

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

References:

BID: <http://www.securityfocus.com/bid/7385>

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-068.msp>

MISC: <http://www.securityfocus.com/data/vulnerabilities/exploits/backrush.patch.README>

MISC: <http://www.securityfocus.com/data/vulnerabilities/exploits/backrush.patch>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/3110>

SECTRAK: <http://securitytracker.com/id?1021163>

SECUNIA: <http://secunia.com/advisories/32633>

CVE Reference: [CVE-2008-4037](http://cve.mitre.org)

- **CVE-2008-5026 Microsoft CVSS 2.0 Score = 4.3**

Microsoft SharePoint uses URLs with the same hostname and port number for a web site's primary files and individual users' uploaded files (aka attachments), which allows remote authenticated users to leverage same-origin relationships and conduct cross-site scripting (XSS) attacks by uploading HTML documents.

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

References:

MISC: http://www.pomcor.com/whitepapers/file_sharing_security.pdf

BUGTRAQ: <http://archives.neohapsis.com/archives/bugtraq/2008-11/0058.html>

BUGTRAQ: <http://archives.neohapsis.com/archives/bugtraq/2008-11/0056.html>

BUGTRAQ: <http://archives.neohapsis.com/archives/bugtraq/2008-11/0055.html>

CVE Reference: [CVE-2008-5026](http://cve.mitre.org)

- **CVE-2008-4029 Microsoft CVSS 2.0 Score = 4.3**

Cross-domain vulnerability in Microsoft XML Core Services 3.0 and 4.0, as used in Internet Explorer, allows remote attackers to obtain sensitive information from another domain via a crafted XML document, related to improper error checks for external DTDs, aka "MSXML DTD Cross-Domain Scripting Vulnerability."

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

References:

BID: <http://www.securityfocus.com/bid/32155>

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-069.msp>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/3111>

SECTRAK: <http://securitytracker.com/id?1021164>

CVE Reference: [CVE-2008-4029](#)

• **CVE-2008-4033 Microsoft CVSS 2.0 Score = 4.3**

Cross-domain vulnerability in Microsoft XML Core Services 3.0 through 6.0, as used in Microsoft Expression Web, Office, Internet Explorer, and other products, allows remote attackers to obtain sensitive information from another domain and corrupt the session state via HTTP request header fields, as demonstrated by the Transfer-Encoding field, aka "MSXML Header Request Vulnerability."

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

References:

BID: <http://www.securityfocus.com/bid/32204>

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-069.msp>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/3111>

SECTRAK: <http://securitytracker.com/id?1021164>

CVE Reference: [CVE-2008-4033](#)

• **CVE-2008-5044 Microsoft CVSS 2.0 Score = 4.0**

Race condition in Microsoft Windows Server 2003 and Vista allows local users to cause a denial of service (crash or hang) via a multi-threaded application that makes many calls to UnhookWindowsHookEx while certain other desktop activity is occurring.

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

References:

BID: <http://www.securityfocus.com/bid/32206>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/498165/100/0/threaded>

MISC: <http://killprog.com/whk.zip>

CVE Reference: [CVE-2008-5044](#)

• **CVE-2008-5035 IBM CVSS 2.0 Score = 5.0**

The Resource Monitoring and Control (RMC) daemon in IBM Hardware Management Console (HMC) 7 release 3.2.0 SP1 and 3.3.0 SP2 allows remote attackers to cause a denial of service (daemon crash or hang) via a packet with an invalid length.

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

References:

CONFIRM: <https://www14.software.ibm.com/webapp/set2/sas/f/hmc/power6/install/v7.Readme.html#MH01134>

CONFIRM: <https://www14.software.ibm.com/webapp/set2/sas/f/hmc/power6/install/v7.Readme.html#MH01133>

XF: <http://xforce.iss.net/xforce/xfdb/46413>

CONFIRM: <http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcמיד?mode=18&ID=4442>

CONFIRM: <http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcמיד?mode=18&ID=4441>

BID: <http://www.securityfocus.com/bid/32181>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/3051>

SECUNIA: <http://secunia.com/advisories/32571>

CVE Reference: [CVE-2008-5035](#)

• **CVE-2008-5014 Mozilla CVSS 2.0 Score = 10.0**

jslock.cpp in Mozilla Firefox 3.x before 3.0.2, Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by modifying the window.__proto__.__proto__ object in a way that causes a lock on a non-native object, which triggers an assertion failure related to the OBJ_IS_NATIVE function.

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

References:

MISC: https://bugzilla.mozilla.org/show_bug.cgi?id=436741

CONFIRM: <http://www.mozilla.org/security/announce/2008/mfsa2008-50.html>

CVE Reference: [CVE-2008-5014](#)

• **CVE-2008-5017 Mozilla CVSS 2.0 Score = 10.0**

Integer overflow in xpccom/io/nsEscape.cpp in the browser engine in Mozilla Firefox 3.x before 3.0.4, Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to cause a denial of service (crash) via unknown vectors.

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

References:

MISC: https://bugzilla.mozilla.org/show_bug.cgi?id=455987

CONFIRM: <http://www.mozilla.org/security/announce/2008/mfsa2008-52.html>

CVE Reference: [CVE-2008-5017](#)

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