ScoutNews
The weekly Security update from the makers of SecureScout
February 27, 2009

2009 Issue #9

Table of Contents

Product Focus

ASN.1 Vulnerability Scanner - The S4 ASN.1 Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the MS04-007 that could allow remote code execution.

Download Here:
http://www.netvigilance.com/productdownloads?productname=asn.1vulnerabilityscanner

This Week in Review

US money for security. Laid-off'ers steal data. Cloud computing has privacy issues. Vandalism still a driver in cyber crime.

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

- **Obama\'s budget proposal increases spending for cybersecurity**

President Obama is asking for $355 million in next year's budget to fund the Department of Homeland Security's (DHS) cybersecurity work.

The funds will be used to "support the base operations of the National Cyber Security Division, as well as initiatives under the Comprehensive National Cybersecurity Initiative (CNCI) to protect our information networks," according to the document.

In fiscal year 2009, cybersecurity under DHS was budgeted at $313.5 million, including $254.9 million for the department's share of CNCI, a largely secretive initiative proposed in January 2008 by President Bush.

SC Magazine

Full Story :
http://www.scmagazineus.com/Obamas-budget-proposal-increases-spending-for-cybersecurity/article/127944/

- **Insider data theft exacerbated by economic crisis**

Updated Tuesday, Feb. 25, 2009 at 11:05 a.m. EST

The majority of individualslaid off, fired or changing jobs in the last 12 months stole data from their former employer, according to a new survey from the Ponemon Institute and Symantec.

Some 945 individuals in the United States who were fired or left their job willingly were surveyed and 59 percent admitted to taking company information when leaving. And it seems, according to the survey, email lists are most susceptible to theft. Typically, a bad impression of the company increased the odds of theft; few companies are taking the proper steps to prevent this problem, the survey found. Further, a portion of companies did not revoke employee access to computer systems right away, Larry Ponemon, chairman and founder of the Ponemon Institute, told SCMagazineUS.com Monday.

SC Magazine

Full Story :
http://www.scmagazineus.com/Insider-data-theft-exacerbated-by-economic-crisis/article/127801/

- **Report cites potential privacy gotchas in cloud computing**

February 25, 2009 (Computerworld) Companies looking to reduce their IT costs and complexity by tapping into cloud computing services should first make sure that they won't be stepping on any privacy land mines in the process, according to a report released this week by the World Privacy Forum.

"There are a whole lot of companies out there that are not thinking about privacy" when they consider cloud computing, said Pam Dixon, executive director of the Cardiff, Calif.-based privacy advocacy group. "You shouldn't be putting consumer data in the cloud until you've done a thorough [privacy] review."

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9128636&source=rss_topic1

- **Study: Hackers still driven by urge to vandalize Web sites**

February 26, 2009 (IDG News Service) A study of 57 Web-site hacks carried out last year showed that the largest block of them — 14, or 24% — were aimed at defacing sites rather than seeking financial gain or causing monetary losses to the organization being attacked.

"While financial gain is certainly a big driver for Web hacking, ideological hacking cannot be ignored," said the report, which was sponsored by Breach Security Inc., a Carlsbad, Calif.-based security software vendor, and prepared with support from the WASC.

Most of the Web-site defacements among the studied attacks "were of a political nature, targeting political parties, candidates and government departments, often with a very specific message related to a campaign," the report said. "Others [had] a cultural aspect, mainly Islamic hackers defacing Western Web sites."

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9128681&source=rss_topic1

New Vulnerabilities Tested in SecureScout

- **14496 Adobe Acrobat / Reader util.printf JavaScript function Vulnerability (Remote File Checking)**

Stack-based buffer overflow in Adobe Acrobat and Reader 8.1.2 and earlier allows remote attackers to execute arbitrary code via a PDF file that calls the util.printf JavaScript function with a crafted format string argument, a related issue to CVE-2008-1104.

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

References:

* BUGTRAQ: 20081104 CORE-2008-0526: Adobe Reader Javascript Printf Buffer Overflow
http://www.securityfocus.com/archive/1/archive/1/498032/100/0/threaded
* BUGTRAQ: 20081104 Secunia Research: Adobe Acrobat/Reader "util.printf()" Buffer Overflow
http://www.securityfocus.com/archive/1/archive/1/498027/100/0/threaded
* BUGTRAQ: 20081104 ZDI-08-072: Adobe Acrobat PDF Javascript printf Stack Overflow Vulnerability

http://www.securityfocus.com/archive/1/archive/1/498055/100/0/threaded
* MILW0RM: 6994
http://www.milw0rm.com/exploits/6994
* MILW0RM: 7006
http://www.milw0rm.com/exploits/7006
* MISC:
http://secunia.com/secunia_research/2008-14/
* MISC:
http://www.coresecurity.com/content/adobe-reader-buffer-overflow
* MISC:
http://www.zerodayinitiative.com/advisories/ZDI-08-072/
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb08-19.html
* REDHAT: RHSA-2008:0974
http://www.redhat.com/support/errata/RHSA-2008-0974.html
* SUSE: SUSE-SR:2008:026
http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00002.html
* CERT: TA08-309A
http://www.us-cert.gov/cas/techalerts/TA08-309A.html
* BID: 32091
http://www.securityfocus.com/bid/32091
* BID: 30035
http://www.securityfocus.com/bid/30035
* FRSIRT: ADV-2008-3001
http://www.frsirt.com/english/advisories/2008/3001
* FRSIRT: ADV-2009-0098
http://www.frsirt.com/english/advisories/2009/0098
* OSVDB: 49520
http://osvdb.org/49520
* SECUNIA: 29773
http://secunia.com/advisories/29773
* SECUNIA: 32872
http://secunia.com/advisories/32872
* SECUNIA: 32700
http://secunia.com/advisories/32700
* SREASON: 4549
http://securityreason.com/securityalert/4549

CVE Reference:

CVE-2008-2992 (cve.mitre.org, nvd.nist.gov)

• 14497 Adobe Acrobat / Reader Array index error Vulnerability (Remote File Checking)

Array index error in Adobe Reader and Acrobat, and the Explorer extension (aka AcroRd32Info), 8.1.2, 8.1.1, and earlier allows remote attackers to execute arbitrary code via a crafted PDF document that triggers an out-of-bounds write, related to parsing of Type 1 fonts.

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

References:

* IDEFENSE: 20081104 Adobe Reader Embedded Font Handling Out of Bounds Array Indexing Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=755
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb08-19.html
* REDHAT: RHSA-2008:0974
http://www.redhat.com/support/errata/RHSA-2008-0974.html
* SUSE: SUSE-SR:2008:026
http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00002.html
* CERT: TA08-309A
http://www.us-cert.gov/cas/techalerts/TA08-309A.html
* BID: 32100
http://www.securityfocus.com/bid/32100
* FRSIRT: ADV-2008-3001
http://www.frsirt.com/english/advisories/2008/3001
* FRSIRT: ADV-2009-0098
http://www.frsirt.com/english/advisories/2009/0098
* SECUNIA: 32872
http://secunia.com/advisories/32872
* SECUNIA: 32700

http://secunia.com/advisories/32700

CVE Reference:

CVE-2008-4812 (cve.mitre.org, nvd.nist.gov)

• 14498 Adobe Acrobat / Reader long string argument to AcroJS functionVulnerability (Remote File Checking)

The Download Manager in Adobe Acrobat Professional and Reader 8.1.2 and earlier allows remote attackers to execute arbitrary code via a crafted PDF document that calls an AcroJS function with a long string argument, triggering heap corruption.

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

References:

* IDEFENSE: 20081104 Adobe Acrobat Professional And Reader AcroJS Heap Corruption Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=756
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb08-19.html
* REDHAT: RHSA-2008:0974
http://www.redhat.com/support/errata/RHSA-2008-0974.html
* SUSE: SUSE-SR:2008:026
http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00002.html
* CERT: TA08-309A
http://www.us-cert.gov/cas/techalerts/TA08-309A.html
* FRSIRT: ADV-2008-3001
http://www.frsirt.com/english/advisories/2008/3001
* FRSIRT: ADV-2009-0098
http://www.frsirt.com/english/advisories/2009/0098
* OSVDB: 49541
http://osvdb.org/49541
* SECUNIA: 32872
http://secunia.com/advisories/32872
* SECUNIA: 32700
http://secunia.com/advisories/32700

CVE Reference:

CVE-2008-4817 (cve.mitre.org, nvd.nist.gov)

• 14499 Adobe Acrobat / Reader Collab object or malformed PDF memory corruption Vulnerability (Remote File Checking)

Adobe Reader and Acrobat 8.1.2 and earlier allow remote attackers to execute arbitrary code via a crafted PDF document that (1) performs unspecified actions on a Collab object that trigger memory corruption, related to a GetCosObj method; or (2) contains a malformed PDF object that triggers memory corruption during parsing.

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

References:

* BUGTRAQ: 20081104 ZDI-08-073: Adobe Acrobat Reader Malformed PDF Code Execution Vulnerability
http://www.securityfocus.com/archive/1/archive/1/498056/100/0/threaded
* BUGTRAQ: 20081104 ZDI-08-074: Adobe Acrobat PDF Javascript getCosObj Memory Corruption Vulnerability
http://www.securityfocus.com/archive/1/archive/1/498057/100/0/threaded
* MISC:
http://www.zerodayinitiative.com/advisories/ZDI-08-073/
* MISC:
http://www.zerodayinitiative.com/advisories/ZDI-08-074/
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb08-19.html
* REDHAT: RHSA-2008:0974
http://www.redhat.com/support/errata/RHSA-2008-0974.html
* SUSE: SUSE-SR:2008:026
http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00002.html
* CERT: TA08-309A
http://www.us-cert.gov/cas/techalerts/TA08-309A.html
* BID: 32100
http://www.securityfocus.com/bid/32100
* FRSIRT: ADV-2008-3001
http://www.frsirt.com/english/advisories/2008/3001

* FRSIRT: ADV-2009-0098
http://www.frsirt.com/english/advisories/2009/0098
* SECUNIA: 32872
http://secunia.com/advisories/32872
* SECUNIA: 32700
http://secunia.com/advisories/32700
* SREASON: 4564
http://securityreason.com/securityalert/4564

CVE Reference:

CVE-2008-4813 (cve.mitre.org, nvd.nist.gov)

• 14500 Adobe Acrobat / Reader malformed PDF arbitrary code execution Vulnerability (Remote File Checking)

Adobe Acrobat Reader 8.1.2 and earlier allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a malformed PDF document, as demonstrated by 2008-HI2.pdf.

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

References:

* MILW0RM: 5687
http://www.milw0rm.com/exploits/5687
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb08-19.html
* REDHAT: RHSA-2008:0974
http://www.redhat.com/support/errata/RHSA-2008-0974.html
* SUSE: SUSE-SR:2008:026
http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00002.html
* CERT: TA08-309A
http://www.us-cert.gov/cas/techalerts/TA08-309A.html
* BID: 29420
http://www.securityfocus.com/bid/29420
* FRSIRT: ADV-2008-3001
http://www.frsirt.com/english/advisories/2008/3001
* FRSIRT: ADV-2009-0098
http://www.frsirt.com/english/advisories/2009/0098
* SECUNIA: 32872
http://secunia.com/advisories/32872
* SECUNIA: 32700
http://secunia.com/advisories/32700
* XF: acrobatreader-pdf-dos(42886)
http://xforce.iss.net/xforce/xfdb/42886

CVE Reference:

CVE-2008-2549 (cve.mitre.org, nvd.nist.gov)

• 14501 Adobe Acrobat / Reader input validation issue Vulnerability (Remote File Checking)

Unspecified vulnerability in a JavaScript method in Adobe Reader and Acrobat 8.1.2 and earlier allows remote attackers to execute arbitrary code via unknown vectors, related to an "input validation issue."

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

References:

* MISC:
http://www.skyrecon.com/index.php?option=com_content&task=view&id=302&Itemid=124
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb08-19.html
* REDHAT: RHSA-2008:0974
http://www.redhat.com/support/errata/RHSA-2008-0974.html
* SUSE: SUSE-SR:2008:026
http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00002.html
* CERT: TA08-309A
http://www.us-cert.gov/cas/techalerts/TA08-309A.html
* BID: 32100
http://www.securityfocus.com/bid/32100
* FRSIRT: ADV-2008-3001
http://www.frsirt.com/english/advisories/2008/3001

* FRSIRT: ADV-2009-0098
http://www.frsirt.com/english/advisories/2009/0098
* SECUNIA: 32872
http://secunia.com/advisories/32872
* SECUNIA: 32700
http://secunia.com/advisories/32700

CVE Reference:

CVE-2008-4814 (cve.mitre.org, nvd.nist.gov)

• 14502 Adobe Acrobat / Reader Untrusted search path, privileges escalation Vulnerability (Remote File Checking)

Untrusted search path vulnerability in Adobe Reader and Acrobat 8.1.2 and earlier on Unix and Linux allows attackers to gain privileges via a Trojan Horse program in an unspecified directory that is associated with an insecure RPATH.

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

References:

* MISC:
https://bugzilla.redhat.com/show_bug.cgi?id=469882
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb08-19.html
* REDHAT: RHSA-2008:0974
http://www.redhat.com/support/errata/RHSA-2008-0974.html
* SUSE: SUSE-SR:2008:026
http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00002.html
* CERT: TA08-309A
http://www.us-cert.gov/cas/techalerts/TA08-309A.html
* BID: 32100
http://www.securityfocus.com/bid/32100
* FRSIRT: ADV-2008-3001
http://www.frsirt.com/english/advisories/2008/3001
* FRSIRT: ADV-2009-0098
http://www.frsirt.com/english/advisories/2009/0098
* SECUNIA: 32872
http://secunia.com/advisories/32872
* SECUNIA: 32700
http://secunia.com/advisories/32700

CVE Reference:

CVE-2008-4815 (cve.mitre.org, nvd.nist.gov)

• 14503 Adobe Acrobat / Reader Download Manager unspecified Vulnerability (Remote File Checking)

Unspecified vulnerability in the Download Manager in Adobe Reader 8.1.2 and earlier on Windows allows remote attackers to change Internet Security options on a client machine via unknown vectors.

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

References:

* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb08-19.html
* SUSE: SUSE-SR:2008:026
http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00002.html
* CERT: TA08-309A
http://www.us-cert.gov/cas/techalerts/TA08-309A.html
* FRSIRT: ADV-2008-3001
http://www.frsirt.com/english/advisories/2008/3001
* SECUNIA: 32872
http://secunia.com/advisories/32872

CVE Reference:

CVE-2008-4816 (cve.mitre.org, nvd.nist.gov)

• 18279 Wireshark Buffer overflow in wiretap/netscreen.c Vulnerability (Remote File Checking)

Buffer overflow in wiretap/netscreen.c in Wireshark 0.99.7 through 1.0.5 allows user-assisted remote attackers to cause a denial of service (application crash) via a malformed NetScreen snoop file.

The vulnerability is reported in versions 0.99.7 to 1.0.5.

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

References:

* CONFIRM:
http://www.wireshark.org/security/wnpa-sec-2009-01.html
* CONFIRM:
https://bugs.wireshark.org/bugzilla/attachment.cgi?id=2590
* BID: 33690
http://www.securityfocus.com/bid/33690
* FRSIRT: ADV-2009-0370
http://www.frsirt.com/english/advisories/2009/0370
* OSVDB: 51815
http://osvdb.org/51815
* SECUNIA: 33872
http://secunia.com/advisories/33872

CVE Reference:

CVE-2009-0599 (cve.mitre.org, nvd.nist.gov)

- **18280 Wireshark Tektronix K12 dissector denial of service Vulnerability (Remote File Checking)**

Wireshark 0.99.6 through 1.0.5 allows user-assisted remote attackers to cause a denial of service (application crash) via a crafted Tektronix K12 text capture file, as demonstrated by a file with exactly one frame.

The vulnerability is reported in versions 0.99.6 to 1.0.5.

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

References:

* CONFIRM:
http://www.wireshark.org/security/wnpa-sec-2009-01.html
* CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=1937
* BID: 33690
http://www.securityfocus.com/bid/33690
* FRSIRT: ADV-2009-0370
http://www.frsirt.com/english/advisories/2009/0370
* SECUNIA: 33872
http://secunia.com/advisories/33872

CVE Reference:

CVE-2009-0600 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2009-0238 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office Excel 2000 SP3, 2002 SP3, 2003 SP3, and 2007 SP1; Excel Viewer 2003 Gold and SP3; Excel Viewer; Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1; and Excel in Microsoft Office 2004 and 2008 for Mac allow remote attackers to execute arbitrary code via a crafted Excel document that triggers an access attempt on an invalid object, as exploited in the wild in February 2009 by Trojan.Mdropper.AC.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/48875

MISC: http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-022310-4202-99

BID: http://www.securityfocus.com/bid/33870

CONFIRM: http://www.microsoft.com/technet/security/advisory/968272.mspx

SECTRACK: http://securitytracker.com/id?1021744

MISC: http://isc.sans.org/diary.html?storyid=5923

MISC: http://blogs.zdnet.com/security/?p=2658

CVE Reference: CVE-2009-0238

- **CVE-2007-5289 HP CVSS 2.0 Score = 7.6**

HP Mercury Quality Center (QC) 9.2 and earlier, and possibly TestDirector, relies on cached client-side scripts to implement "workflow" and decisions about the "capability" of a user, which allows remote attackers to execute arbitrary code via crafted use of the Open Test Architecture (OTA) API, as demonstrated by modifying (1) common.tds, (2) defects.tds, (3) manrun.tds, (4) req.tds, (5) testlab.tds, or (6) testplan.tds in %tmp%\TD_80, and then setting the file's properties to read-only.

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

References:

CERT-VN: http://www.kb.cert.org/vuls/id/898865

XF: http://xforce.iss.net/xforce/xfdb/48860

BID: http://www.securityfocus.com/bid/33854

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/501177/100/0/threaded

SECUNIA: http://secunia.com/advisories/34015

MISC: http://blogs.exposit.co.uk/2009/02/23/vulnerability-in-quality-center/

CVE Reference: CVE-2007-5289

- **CVE-2009-0505 IBM CVSS 2.0 Score = 9.0**

The CICS listener in IBM TXSeries for Multiplatforms 6.2 GA waits for a forcepurge acknowledgement from the CICS Application Server (CICSAS) after an eci response timeout, which might allow remote authenticated users to cause a denial of service (forcepurge handling delay), or have unspecified other impact, via vectors involving slow or nonexistent acknowledgement.

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

References:

CONFIRM: http://www-01.ibm.com/support/docview.wss?uid=swg24019725

XF: http://xforce.iss.net/xforce/xfdb/48885

BID: http://www.securityfocus.com/bid/33883

CVE Reference: CVE-2009-0505

- **CVE-2009-0439 IBM CVSS 2.0 Score = 7.2**

Unspecified vulnerability in the queue manager in IBM WebSphere MQ (WMQ) 5.3, 6.0 before 6.0.2.6, and 7.0 before 7.0.0.2 allows local users to gain privileges via vectors related to the (1) setmqaut, (2) dmpmqaut, and (3) dspmqaut authorization commands.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/48529

MISC: http://www-01.ibm.com/support/docview.wss?rs=171&uid=swg27006037

BID: http://www.securityfocus.com/bid/33857

CVE Reference: CVE-2009-0439

- **CVE-2009-0440 IBM CVSS 2.0 Score = 6.5**

IBM WebSphere Partner Gateway (WPG) 6.0.0 through 6.0.0.7 does not properly handle failures of signature verification, which might allow remote authenticated users to submit a crafted RosettaNet (aka RNIF) document to a backend application, related to (1) "altered service content" and (2) "digital signature foot-print."

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

References:

CONFIRM: http://www-01.ibm.com/support/docview.wss?uid=swg21330341

XF: http://xforce.iss.net/xforce/xfdb/48530

BID: http://www.securityfocus.com/bid/33839

AIXAPAR: http://www-1.ibm.com/support/docview.wss?uid=swg1JR31231

SECUNIA: http://secunia.com/advisories/33994

CVE Reference: CVE-2009-0440

- **CVE-2009-0506 IBM CVSS 2.0 Score = 6.2**

Unspecified vulnerability in IBM WebSphere Application Server (WAS) 5.1 and 6.0.2 before 6.0.2.33 on z/OS, when CSIv2 Identity Assertion is enabled and Enterprise JavaBeans (EJB) interaction occurs between a WAS 6.1 instance and a WAS pre-6.1 instance, allows local users to have an unknown impact via vectors related to (1) use of the wrong subject and (2) multiple CBIND checks.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/48886

CONFIRM: http://www-01.ibm.com/support/docview.wss?uid=swg27006876

BID: http://www.securityfocus.com/bid/33884

CVE Reference: CVE-2009-0506

- **CVE-2008-6280 Cisco CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in apply.cgi on the Linksys WRT160N allows remote attackers to inject arbitrary web script or HTML via the action parameter in a DHCP_Static operation.

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

References:

BID: http://www.securityfocus.com/bid/32496

SECUNIA: http://secunia.com/advisories/32877

MISC: http://packetstormsecurity.org/0811-exploits/linksys-xss.txt

CVE Reference: CVE-2008-6280

- **CVE-2009-0675 Linux CVSS 2.0 Score = 2.1**

The skfp_ioctl function in drivers/net/skfp/skfddi.c in the Linux kernel before 2.6.28.6 permits SKFP_CLR_STATS requests only when the CAP_NET_ADMIN capability is absent, instead of when this capability is present, which allows local users to reset the driver statistics, related to an "inverted logic" issue.

Test Case Impact: Vulnerability Impact: Risk: **Low**

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=486534

CONFIRM: http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.28.6

SECUNIA: http://secunia.com/advisories/33938

MLIST: http://openwall.com/lists/oss-security/2009/02/20/2

MLIST: http://lists.openwall.net/netdev/2009/01/28/90

CONFIRM: http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=c25b9abbc2c2c0da88e180c3933d6e773245815a

CVE Reference: CVE-2009-0675

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