

2009 Issue #27

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

[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

Russo insists on PCI standard. About the necessity of a CSO. Ethical military robots?? What not to do on social networks.

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

• Q&A: No alternative to PCI, security council chief insists

Computerworld - As the general manager of the Payment Card Industry Security Standards Council, Robert Russo has borne the brunt of criticism about the PCI data security standard. Computerworld spoke with Russo last week as the council prepared to receive formal comments from industry stakeholders about the current version of the standard, which went into effect last fall. Russo stoutly defended the standard and said that despite questions about its effectiveness, there's no alternative when it comes to protecting payment card data.

What do you say to those who have said the PCI rules-making process is not as inclusive as it needs to be? The way it works is after we release a new standard, it stays out there for a approximately eight months and then a new comment period begins. All of our participating organizations, as well as all of the assessment community and approved software vendors and such will have the opportunity to give us formal feedback. We will ask them to tell us what their top five priorities are regarding the standard--what they would like to see addressed, what they'd like to see changed, what they'd like to see added or deleted. We take all of this information and we will digest that and put that in some form that can be distributed once again to the participating communities, saying: 'This is the result of everything we have gotten. And this is what we are proposing, based on what we heard should be in the newest version of the

standard,' and then we will have another comment period. That information will be the basis for the new or evolved standard that will be released. Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9134953>

• **The Cybersecurity Coordinator's Job Description**

CSO - About this series: In a paper he wrote and published before President Obama's announcement regarding the creation of a national cybersecurity coordinator, Ariel Silverstone, a CISSP and former member of the Israeli Defense Forces, put forward his thoughts about the necessity of having a chief security officer for the United States. In this second installment, he discusses where he sees the CSO role fitting in, and the core "Three Tenets" he sees as critical to success in this role. Silverstone also lists his vision for the next 6 (of 23) tasks that he sees as essential for information security in the United States.

READ PART 1: Mission Impossible? A Plan to Secure the Federal Cyberspace Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9135058>

• **CNET News Daily Podcast: On building ethical military robots**

Robotics engineer Ronald Arkin of Georgia Tech just finished a three-year contract with the U.S. Army designing software to create ethical robots. His thesis is that robots can be configured with a built-in "guilt system" that eventually could make them better at avoiding civilian casualties than human soldiers. CNET intern Dara Kerr talks to Arkin about his work.

Also in today's podcast: Jammie Thomas-Rasset's lawyers say she plans to appeal her RIAA case; MySpace--and presumably other community-based Web services--cannot be held liable in assault charges stemming from people meeting on its Web site; and watch out for Waledac over the 4th of July weekend.

Listen now: Download today's podcast Cnet Security

Full Story :

http://news.cnet.com/8301-11424_3-10278435-90.html?part=rss&subj=news&tag=2547-1_3-0-20

• **Seven Deadly Sins of Social Networking Security**

CSO - Admit it: You are currently addicted to social networking. Your drug of choice might be Facebook or Twitter, or maybe Myspace or LinkedIn. Some of you are using all of the above, and using them hard, even IT security practitioners who know better.

While it's impossible to escape every social networking threat out there, there are steps one can take to significantly reduce the risks. CSOonline recently checked in with dozens of IT security professionals (ironically, using more than one social networking platform to do so) to pinpoint seven typical security mistakes people make; and how to avoid them. Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9134994>

• **Net neutrality gets a boost from the feds**

Net neutrality advocates got a boost of support Wednesday from the Obama administration when it released grant guidelines for spending the government's \$7.2 billion broadband stimulus package.

Companies winning grants to help build new broadband infrastructure will have to follow the Federal Communications Commission's Internet Policy statement, which prohibits companies from deliberately blocking or slowing Internet traffic on their networks.

Proponents of that concept, Net neutrality, have been pushing the government to pass laws or set stricter requirements to ensure that consumers get access to content they want and that competitors are not run out of business by network operators. Cnet Security

Full Story :

http://news.cnet.com/8301-1035_3-10278484-94.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• **14508 Adobe Acrobat / Reader PDF file with a malformed JBIG2 symbol dictionary segment, heap-based buffer overflow Vulnerability (Remote File Checking)**

Heap-based buffer overflow in Adobe Acrobat Reader 9 before 9.1, 8 before 8.1.4, and 7 before 7.1.1 allows remote attackers to execute arbitrary code via a PDF file with a malformed JBIG2 symbol dictionary segment, a different vulnerability than CVE-2009-1061 and CVE-2009-1062.

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

References:

- * BUGTRAQ: 20090325 Secunia Research: Adobe Reader JBIG2 Symbol Dictionary Buffer Overflow
<http://www.securityfocus.com/archive/1/archive/1/502155/100/0/threaded>
- * MISC:
http://secunia.com/secunia_research/2009-14/
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-04.html>
- * GENTOO: GLSA-200904-17
<http://security.gentoo.org/glsa/glsa-200904-17.xml>
- * REDHAT: RHSA-2009:0376
<http://www.redhat.com/support/errata/RHSA-2009-0376.html>
- * SUNALERT: 256788
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-256788-1>
- * SUSE: SUSE-SA:2009:014
<http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00005.html>
- * SUSE: SUSE-SR:2009:009
<http://lists.opensuse.org/opensuse-security-announce/2009-04/msg00010.html>
- * BID: 34229
<http://www.securityfocus.com/bid/34229>
- * SECTRACK: 1021892
<http://www.securitytracker.com/id?1021892>
- * SECUNIA: 34392
<http://secunia.com/advisories/34392>
- * SECUNIA: 34490
<http://secunia.com/advisories/34490>
- * SECUNIA: 34706
<http://secunia.com/advisories/34706>
- * SECUNIA: 34790
<http://secunia.com/advisories/34790>
- * VUPEN: ADV-2009-1019
<http://www.vupen.com/english/advisories/2009/1019>

CVE Reference:

CVE-2009-0193 (cve.mitre.org, nvd.nist.gov)

• 14509 Adobe Acrobat / Reader PDF file containing a JBIG2 stream with a size inconsistency related to an unspecified table, heap-based buffer overflow Vulnerability (Remote File Checking)

Heap-based buffer overflow in Adobe Acrobat Reader and Acrobat Professional 7.1.0, 8.1.3, 9.0.0, and other versions allows remote attackers to execute arbitrary code via a PDF file containing a JBIG2 stream with a size inconsistency related to an unspecified table.

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

References:

- * IDEFENSE: 20090324 Adobe Reader and Acrobat JBIG2 Encoded Stream Heap Overflow Vulnerability
<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=776>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-04.html>
- * GENTOO: GLSA-200904-17
<http://security.gentoo.org/glsa/glsa-200904-17.xml>
- * REDHAT: RHSA-2009:0376
<http://www.redhat.com/support/errata/RHSA-2009-0376.html>
- * SUNALERT: 256788
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-256788-1>
- * SUSE: SUSE-SA:2009:014
<http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00005.html>
- * SUSE: SUSE-SR:2009:009
<http://lists.opensuse.org/opensuse-security-announce/2009-04/msg00010.html>
- * BID: 34229
<http://www.securityfocus.com/bid/34229>
- * SECTRACK: 1021892
<http://www.securitytracker.com/id?1021892>

* SECUNIA: 34392
<http://secunia.com/advisories/34392>
* SECUNIA: 34490
<http://secunia.com/advisories/34490>
* SECUNIA: 34706
<http://secunia.com/advisories/34706>
* SECUNIA: 34790
<http://secunia.com/advisories/34790>
* VUPEN: ADV-2009-1019
<http://www.vupen.com/english/advisories/2009/1019>

CVE Reference:

CVE-2009-0928 (cve.mitre.org, nvd.nist.gov)

• 14510 Adobe Acrobat / Reader PDF file containing a JBIG2 stream, arbitrary code execution Vulnerability (CVE-2009-1061) (Remote File Checking)

Unspecified vulnerability in Adobe Acrobat Reader 9 before 9.1, 8 before 8.1.4, and 7 before 7.1.1 might allow remote attackers to execute arbitrary code via unknown attack vectors related to JBIG2 and "input validation," a different vulnerability than CVE-2009-0193 and CVE-2009-1062.

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

References:

* CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-04.html>
* GENTOO: GLSA-200904-17
<http://security.gentoo.org/glsa/glsa-200904-17.xml>
* REDHAT: RHSA-2009:0376
<http://www.redhat.com/support/errata/RHSA-2009-0376.html>
* SUNALERT: 256788
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-256788-1>
* SUSE: SUSE-SA:2009:014
<http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00005.html>
* SUSE: SUSE-SR:2009:009
<http://lists.opensuse.org/opensuse-security-announce/2009-04/msg00010.html>
* BID: 34229
<http://www.securityfocus.com/bid/34229>
* SECTRACK: 1021892
<http://www.securitytracker.com/id?1021892>
* SECUNIA: 34392
<http://secunia.com/advisories/34392>
* SECUNIA: 34490
<http://secunia.com/advisories/34490>
* SECUNIA: 34706
<http://secunia.com/advisories/34706>
* SECUNIA: 34790
<http://secunia.com/advisories/34790>
* VUPEN: ADV-2009-1019
<http://www.vupen.com/english/advisories/2009/1019>

CVE Reference:

CVE-2009-1061 (cve.mitre.org, nvd.nist.gov)

• 14511 Adobe Acrobat / Reader PDF file containing a JBIG2 stream, arbitrary code execution Vulnerability (Remote File Checking)

Adobe Acrobat Reader 9 before 9.1, 8 before 8.1.4, and 7 before 7.1.1 might allow remote attackers to trigger memory corruption and possibly execute arbitrary code via unknown attack vectors related to JBIG2, a different vulnerability than CVE-2009-0193 and CVE-2009-1061.

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

References:

* MISC:
<http://www.ivizsecurity.com/security-advisory-iviz-sr-09001.html>
* CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-04.html>
* GENTOO: GLSA-200904-17

<http://security.gentoo.org/glsa/glsa-200904-17.xml>

* REDHAT: RHSA-2009:0376

<http://www.redhat.com/support/errata/RHSA-2009-0376.html>

* SUNALERT: 256788

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-256788-1>

* SUSE: SUSE-SA:2009:014

<http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00005.html>

* SUSE: SUSE-SR:2009:009

<http://lists.opensuse.org/opensuse-security-announce/2009-04/msg00010.html>

* BID: 34229

<http://www.securityfocus.com/bid/34229>

* SECTRACK: 1021892

<http://www.securitytracker.com/id?1021892>

* SECUNIA: 34392

<http://secunia.com/advisories/34392>

* SECUNIA: 34490

<http://secunia.com/advisories/34490>

* SECUNIA: 34706

<http://secunia.com/advisories/34706>

* SECUNIA: 34790

<http://secunia.com/advisories/34790>

* VUPEN: ADV-2009-1019

<http://www.vupen.com/english/advisories/2009/1019>

CVE Reference:

CVE-2009-1062 (cve.mitre.org, nvd.nist.gov)

• 14512 Adobe Acrobat / Reader JBIG2 filter memory corruption Vulnerability (Remote File Checking)

Heap-based buffer overflow in the JBIG2 filter in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a crafted PDF file that contains JBIG2 text region segments with Huffman encoding.

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

References:

* BUGTRAQ: 20090610 Secunia Research: Adobe Reader JBIG2 Text Region Segment Buffer Overflow

<http://www.securityfocus.com/archive/1/archive/1/504217/100/0/threaded>

* MISC:

http://secunia.com/secunia_research/2009-24/

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb09-07.html>

* REDHAT: RHSA-2009:1109

<http://www.redhat.com/support/errata/RHSA-2009-1109.html>

* CERT: TA09-161A

<http://www.us-cert.gov/cas/techalerts/TA09-161A.html>

* BID: 35274

<http://www.securityfocus.com/bid/35274>

* BID: 35302

<http://www.securityfocus.com/bid/35302>

* SECTRACK: 1022361

<http://securitytracker.com/id?1022361>

* SECUNIA: 34580

<http://secunia.com/advisories/34580>

* SECUNIA: 35496

<http://secunia.com/advisories/35496>

* VUPEN: ADV-2009-1547

<http://www.vupen.com/english/advisories/2009/1547>

* XF: reader-acrobat-jbig2-code-exec(51015)

<http://xforce.iss.net/xforce/xfdb/51015>

CVE Reference:

CVE-2009-0198 (cve.mitre.org, nvd.nist.gov)

• 18214 Insecure protocol FTP running

FTP transmits data and passwords in clear text, and should only be used for non-sensitive information. Avoid using FTP passwords on other systems. It is recommended to use FTPs (FTP/SSL) or SSH/SCP instead.

PCI requires that all insecure protocol be disabled to ensures that cardholder data is safe as per PCI DSS version 1.2 Requirement 2.2.2.

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

References:

* MISC: About the PCI Data Security Standard (PCI DSS)
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

CVE Reference:

CVE-1999-0614 (cve.mitre.org, nvd.nist.gov)

● **18362 Web Proxy TCP State Limited Denial of Service Vulnerability (MS09-016/961759) (Remote File Checking)**

A denial of service vulnerability exists in the way the firewall engine handles TCP state for Web proxy or Web publishing listeners. The vulnerability could allow a remote user to cause a Web listener to stop responding to new requests.

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

References:

* MS: MS09-016
<http://www.microsoft.com/technet/security/Bulletin/MS09-016.msp>
* CERT: TA09-104A
<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>
* OSVDB: 53636
<http://osvdb.org/53636>
* SECTRACK: 1022045
<http://www.securitytracker.com/id?1022045>
* SECUNIA: 34687
<http://secunia.com/advisories/34687>
* VUPEN: ADV-2009-1030
<http://www.vupen.com/english/advisories/2009/1030>

CVE Reference:

CVE-2009-0077 (cve.mitre.org, nvd.nist.gov)

● **18363 Cross-Site Scripting Vulnerability (MS09-016/961759) (Remote File Checking)**

A cross-site scripting (XSS) vulnerability exists in the HTML forms authentication component in ISA Server or Forefront TMG, cookieauth.dll, which could allow malicious script code to run on the machine of another user under the guise of the server running cookieauth.dll. This is a non-persistent cross-site scripting vulnerability that can lead to spoofing and information disclosure.

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

References:

* MS: MS09-016
<http://www.microsoft.com/technet/security/Bulletin/MS09-016.msp>
* CERT: TA09-104A
<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>
* OSVDB: 53637
<http://osvdb.org/53637>
* SECTRACK: 1022046
<http://www.securitytracker.com/id?1022046>
* SECUNIA: 34687
<http://secunia.com/advisories/34687>
* VUPEN: ADV-2009-1030
<http://www.vupen.com/english/advisories/2009/1030>

CVE Reference:

CVE-2009-0237 (cve.mitre.org, nvd.nist.gov)

● **18427 Microsoft Works File Converter Buffer Overflow Vulnerability (MS09-024/957632) (Remote File Checking)**

A remote code execution vulnerability exists in the way that the Works for Windows document converters handle specially crafted Works files. The vulnerability could allow remote code execution if a user opens a specially crafted .wps file. 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:

- * MISC:
<http://blogs.technet.com/srd/archive/2009/06/09/ms09-024.aspx>
- * MS: MS09-024
<http://www.microsoft.com/technet/security/Bulletin/MS09-024.msp>
- * JVN: JVN#70858401
<http://jvn.jp/en/jp/JVN70858401/index.html>
- * BID: 35184
<http://www.securityfocus.com/bid/35184>
- * OSVDB: 54939
<http://osvdb.org/54939>
- * SECTRACK: 1022354
<http://www.securitytracker.com/id?1022354>
- * SECTRACK: 1022355
<http://www.securitytracker.com/id?1022355>
- * SECUNIA: 35371
<http://secunia.com/advisories/35371>
- * VUPEN: ADV-2009-1543
<http://www.vupen.com/english/advisories/2009/1543>

CVE Reference:

CVE-2009-1533 (cve.mitre.org, nvd.nist.gov)

• 18435 Script Execution in Windows Search Vulnerability (MS09-023/963093) (Remote File Checking)

An information disclosure vulnerability exists in Windows Search due to the way file previews are generated. Attempts to exploit this vulnerability require user interaction. An attacker who successfully exploited this vulnerability could run a malicious HTML script that could disclose information, forward user data to a third party, or access any data on the affected systems that was accessible to the logged-on user. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly, but it could be used to produce information that could be used to try to further compromise the affected system.

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

References:

- * MS: MS09-023
<http://www.microsoft.com/technet/security/Bulletin/MS09-023.msp>
- * OSVDB: 54935
<http://osvdb.org/54935>
- * SECTRACK: 1022353
<http://www.securitytracker.com/id?1022353>
- * SECUNIA: 35366
<http://secunia.com/advisories/35366>
- * VUPEN: ADV-2009-1542
<http://www.vupen.com/english/advisories/2009/1542>

CVE Reference:

CVE-2009-0239 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-2298 HP CVSS 2.0 Score = 7.5

Stack-based buffer overflow in rping in HP OpenView Network Node Manager (OV NNM) 7.53 on Linux allows remote attackers to execute arbitrary code via unspecified vectors, possibly involving a CGI request to webappmon.exe. NOTE: this may overlap CVE-2009-1420.

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

References:

IDEFENSE: <http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=810>

CVE Reference: [CVE-2009-2298](#)

• CVE-2009-1421 HP CVSS 2.0 Score = 2.1

Unspecified vulnerability in NFS / ONCplus on HP HP-UX B.11.31 allows local users to cause a denial of service via unknown attack vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.

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

References:

BID: <http://www.securityfocus.com/bid/35547>

CVE Reference: [CVE-2009-1421](#)

• CVE-2009-2296 Sun CVSS 2.0 Score = 10.0

The NFSv4 server kernel module in Sun Solaris 10, and OpenSolaris before snv_119, does not properly implement the nfs_portmon setting, which allows remote attackers to access shares, and read, create, and modify arbitrary files, via unspecified vectors.

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

References:

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-66-262668-1>

CONFIRM: <http://sunsolve.sun.com/search/document.do?assetkey=1-21-139991-03-1>

CVE Reference: [CVE-2009-2296](#)

• CVE-2009-2297 Sun CVSS 2.0 Score = 7.1

Unspecified vulnerability in the udp subsystem in the kernel in Sun Solaris 10, and OpenSolaris snv_90 through snv_108, when Solaris Trusted Extensions is enabled, allows remote attackers to cause a denial of service (panic) via unspecified vectors involving the crgetlabel function, related to a "TX panic." NOTE: this issue exists because of a regression in earlier kernel patches.

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

References:

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-66-262048-1>

CONFIRM: <http://sunsolve.sun.com/search/document.do?assetkey=1-21-141414-02-1>

CVE Reference: [CVE-2009-2297](#)

• CVE-2009-2287 Linux CVSS 2.0 Score = 4.9

The kvm_arch_vcpu_ioctl_set_sregs function in the KVM in Linux kernel 2.6 before 2.6.30, when running on x86 systems, does not validate the page table root in a KVM_SET_SREGS call, which allows local users to cause a denial of service (crash or hang) via a crafted cr3 value, which triggers a NULL pointer dereference in the gfn_to_rmap function.

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

References:

MLIST: <http://www.openwall.com/lists/oss-security/2009/06/30/1>

CONFIRM: http://sourceforge.net/tracker/?func=detail&atid=893831&aid=2687641&group_id=180599

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=59839dff5eabca01cc4e20b45797a60a80af8cb>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/stable/stable-queue.git;a=blob:f=queue-2.6.30/kvm-x86-check-for-cr3-validity-in-ioc>

CVE Reference: [CVE-2009-2287](#)

• CVE-2009-2282 Sun CVSS 2.0 Score = 4.6

The Virtual Network Terminal Server daemon (vntsd) for Logical Domains (aka LDoms) in Sun Solaris 10, and OpenSolaris snv_41 through snv_108, on SPARC platforms does not check authorization for guest console access, which allows local control-domain users to gain guest-domain privileges via unknown vectors.

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

References:

CONFIRM: <http://sunsolve.sun.com/search/document.do?assetkey=1-21-141778-01-1>

BID: <http://www.securityfocus.com/bid/35502>

OSVDB: <http://www.osvdb.org/55329>

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-66-262708-1>

SECUNIA: <http://secunia.com/advisories/35547>

CVE Reference: [CVE-2009-2282](#)

• **CVE-2009-2312 McAfee CVSS 2.0 Score = 4.6**

SmartFilter Web Gateway Security 4.2.1.00 stores user credentials in cleartext in config.txt and uses insecure permissions for this file, which allows local users to gain privileges.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/49338>

SECUNIA: <http://secunia.com/advisories/34390>

FULLDISC: <http://archives.neohapsis.com/archives/fulldisclosure/2009-03/0314.html>

CVE Reference: [CVE-2009-2312](#)

• **CVE-2009-2283 Sun CVSS 2.0 Score = 4.3**

Multiple cross-site scripting (XSS) vulnerabilities in the help jsp scripts in Sun Java Web Console 3.0.2 through 3.0.5, and Sun Java Web Console in Solaris 10, allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.

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

References:

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-66-262428-1>

CONFIRM: <http://sunsolve.sun.com/search/document.do?assetkey=1-21-136987-03-1>

CVE Reference: [CVE-2009-2283](#)

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