

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

[Apache Chunked Vulnerability Scanner](#) - The S4 Apache Chunked 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 Apache Chunked Encoding buffer overflow.

Download Here:

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

This Week in Review

Software and security (or not). Recession and temp workers and data security. Cloud Computing Forum says security fears are too heavy. US improved health system and security.

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

• Security Manager's Journal: Another delay is another black eye for security

February 16, 2009 (Computerworld) This week, I ran into unexpected trouble. A project is ready to go live, but it never received a security review. And it has a lot of the elements that would go into a worst-case scenario: a third party, sensitive data, the Internet and no plans for encryption.

Maybe because it's a third-party application that's accessed over the Internet via software on end-user systems. People tend to think of that sort of implementation as a hands-off situation. Of course, most people don't think like a security manager.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=333373&source=rss_topic17

• Recession Makes IAM More Important Than Ever

February 17, 2009 (CSO) Any economic downturn brings new risks to your organization. Nervous employees who fear downsizing may be tempted to gain unauthorized access to sensitive information stored across applications while temporary workers are less loyal and identity verification processes for full-time employees may not be used, making your organization more susceptible.

Security is an issue with temporary employees because although they offer a lower-cost workforce option as they are hired and fired much more easily than permanent employees, they also bring increased risks. They lack the loyalty that permanent employees feel toward the company and may be less inclined to recognize and report inappropriate activities but they need the same thorough vetting and training as permanent employees. And, because their turnover rate is much higher than that of normal employees, temporary workers need to be provisioned and de-provisioned more often, quickly and cost effectively in large numbers.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9128091&source=rss_topic1

• **Cloud security fears called overblown, 'emotional' at IDC forum**

February 18, 2009 (IDG News Service) It may sound like heresy to say it, but it's possible to worry a little too much about security in cloud computing environments, speakers at IDC's Cloud Computing Forum said on Wednesday.

Keeping data secure is critical, of course, but companies need to be realistic about the level of security they achieve inside their own business, and how that might compare to a cloud provider such as Amazon Web Services or Salesforce.com, forum speakers said.

That was the experience of Doug Menefee, CIO at Schumacher Group, which provides emergency-room management services to hospitals. The company is in the midst of a project to migrate most of its applications to hosted, cloud-based services.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9128260&source=rss_topic1

• **Security Challenges of Electronic Medical Records**

February 19, 2009 (CSO) Under his recently unveiled fiscal stimulus plan, President Obama seeks to invest up to US\$20 Billion in federal funds to achieve widespread deployment of Electronic Medical Records (EMRs). A principal reason for his initiative is to improve our nation's health care system by reducing long term costs and increasing effectiveness of our health outlays. So what exactly is an Electronic Medical Record and what does this new direction mean for security and privacy professionals?

The focus of this article, however, is on the secure use of EMRs by institutions and health providers in a regulatory arena rife with complexity and with strict privacy and safety requirements. Consider a typical hospital with a relatively well functioning EMR system. Using EMRs, doctors can conduct much of their business totally electronically. This is in sharp contrast to traditional care environments where paper shuffling is the norm. Using EMRs, doctors can review patient histories and charts, obtain laboratory results, generate referrals for specialist consultations, prescribe medicines, and diagnose images all without the use of paper. This sounds utopian, and in many ways it is.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9128261&source=rss_topic1

New Vulnerabilities Tested in SecureScout

• **16732 Oracle Enterprise Manager - CORE: Repository component unspecified Vulnerability (jul-2006/EM01)**

An unspecified vulnerability with unknown impact exists in Oracle Enterprise Manager CORE: Repository component.

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html>

* MISC:

http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html

* HP: HPSBMA02133
<http://www.securityfocus.com/archive/1/archive/1/440758/100/100/threaded>
* CERT: TA06-200A
<http://www.us-cert.gov/cas/techalerts/TA06-200A.html>
* BID: 19054
<http://www.securityfocus.com/bid/19054>
* FRSIRT: ADV-2006-2863
<http://www.frsirt.com/english/advisories/2006/2863>
* FRSIRT: ADV-2006-2947
<http://www.frsirt.com/english/advisories/2006/2947>
* SECTRACK: 1016529
<http://securitytracker.com/id?1016529>
* SECUNIA: 21111
<http://secunia.com/advisories/21111>
* SECUNIA: 21165
<http://secunia.com/advisories/21165>
* XF: oracle-cpu-july-2006(27897)
<http://xforce.iss.net/xforce/xfdb/27897>

CVE Reference:

CVE-2006-3719 (cve.mitre.org, nvd.nist.gov)

• 18270 Wireshark Bluetooth ACL dissector denial of service Vulnerability (Remote File Checking)

The dissect_btaccl function in packet-bthci_acl.c in the Bluetooth ACL dissector in Wireshark 0.99.2 through 1.0.3 allows remote attackers to cause a denial of service (application crash or abort) via a packet with an invalid length, related to an erroneous tvb_memcpy call.

The vulnerability is reported in versions 0.99.2 to 1.0.3.

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

References:

* BUGTRAQ: 20081211 rPSA-2008-0336-1 tshark wireshark
<http://www.securityfocus.com/archive/1/archive/1/499154/100/0/threaded>
* CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2008-06.html>
* CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=1513
* CONFIRM:
<http://wiki.rpath.com/Advisories:rPSA-2008-0336>
* DEBIAN: DSA-1673
<http://www.debian.org/security/2008/dsa-1673>
* MANDRIVA: MDVSA-2008:215
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:215>
* BID: 31838
<http://www.securityfocus.com/bid/31838>
* FRSIRT: ADV-2008-2872
<http://www.frsirt.com/english/advisories/2008/2872>
* SECTRACK: 1021069
<http://securitytracker.com/id?1021069>
* SECUNIA: 32355
<http://secunia.com/advisories/32355>
* SECUNIA: 32944
<http://secunia.com/advisories/32944>

CVE Reference:

CVE-2008-4683 (cve.mitre.org, nvd.nist.gov)

• 18271 Wireshark Q.931 dissector denial of service Vulnerability (Remote File Checking)

Use-after-free vulnerability in the dissect_q931_cause_ie function in packet-q931.c in the Q.931 dissector in Wireshark 0.10.3 through 1.0.3 allows remote attackers to cause a denial of service (application crash or abort) via certain packets that trigger an exception.

The vulnerability is reported in versions 0.10.3 to 1.0.3.

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

References:

* BUGTRAQ: 20081211 rPSA-2008-0336-1 tshark wireshark
<http://www.securityfocus.com/archive/1/archive/1/499154/100/0/threaded>
* CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2008-06.html>
* CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=2870
* CONFIRM:
<http://wiki.rpath.com/Advisories:rPSA-2008-0336>
* DEBIAN: DSA-1673
<http://www.debian.org/security/2008/dsa-1673>
* MANDRIVA: MDVSA-2008:215
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:215>
* BID: 31838
<http://www.securityfocus.com/bid/31838>
* FRSIRT: ADV-2008-2872
<http://www.frsirt.com/english/advisories/2008/2872>
* SECTRACK: 1021069
<http://securitytracker.com/id?1021069>
* SECUNIA: 32355
<http://secunia.com/advisories/32355>
* SECUNIA: 32944
<http://secunia.com/advisories/32944>

CVE Reference:

CVE-2008-4685 (cve.mitre.org, nvd.nist.gov)

• 18272 Wireshark Tamos CommView dissector denial of service Vulnerability (Remote File Checking)

wtap.c in Wireshark 0.99.7 through 1.0.3 allows remote attackers to cause a denial of service (application abort) via a malformed Tamos CommView capture file (aka .ncf file) with an "unknown/unexpected packet type" that triggers a failed assertion.

The vulnerability is reported in versions 0.99.7 to 1.0.3.

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

References:

* BUGTRAQ: 20081211 rPSA-2008-0336-1 tshark wireshark
<http://www.securityfocus.com/archive/1/archive/1/499154/100/0/threaded>
* MILWORM: 6622
<http://www.milw0rm.com/exploits/6622>
* CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2008-06.html>
* CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=2926
* CONFIRM:
<http://wiki.rpath.com/Advisories:rPSA-2008-0336>
* MANDRIVA: MDVSA-2008:215
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:215>
* BID: 31838
<http://www.securityfocus.com/bid/31838>
* FRSIRT: ADV-2008-2872
<http://www.frsirt.com/english/advisories/2008/2872>
* SECTRACK: 1021069
<http://securitytracker.com/id?1021069>
* SECUNIA: 32355
<http://secunia.com/advisories/32355>
* SREASON: 4462
<http://securityreason.com/securityalert/4462>

CVE Reference:

CVE-2008-4682 (cve.mitre.org, nvd.nist.gov)

• 18273 Wireshark USB dissector denial of service Vulnerability (Remote File Checking)

packet-usb.c in the USB dissector in Wireshark 0.99.7 through 1.0.3 allows remote attackers to cause a denial of service (application crash or abort) via a malformed USB Request Block (URB).

The vulnerability is reported in versions 0.99.7 to 1.0.3.

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

References:

- * BUGTRAQ: 20081211 rPSA-2008-0336-1 tshark wireshark
<http://www.securityfocus.com/archive/1/archive/1/499154/100/0/threaded>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2008-06.html>
- * CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=2922
- * CONFIRM:
<http://wiki.rpath.com/Advisories:rPSA-2008-0336>
- * MANDRIVA: MDVSA-2008:215
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:215>
- * BID: 31838
<http://www.securityfocus.com/bid/31838>
- * FRSIRT: ADV-2008-2872
<http://www.frsirt.com/english/advisories/2008/2872>
- * SECTrack: 1021069
<http://securitytracker.com/id?1021069>
- * SECUNIA: 32355
<http://secunia.com/advisories/32355>

CVE Reference:

CVE-2008-4680 (cve.mitre.org, nvd.nist.gov)

• 18274 Wireshark PRP and MATE dissectors denial of service Vulnerabilities (Remote File Checking)

packet-frame in Wireshark 0.99.2 through 1.0.3 does not properly handle exceptions thrown by post dissectors, which allows remote attackers to cause a denial of service (application crash) via a certain series of packets, as demonstrated by enabling the (1) PRP or (2) MATE post dissector.

The vulnerability is reported in versions 0.99.2 to 1.0.3.

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

References:

- * BUGTRAQ: 20081211 rPSA-2008-0336-1 tshark wireshark
<http://www.securityfocus.com/archive/1/archive/1/499154/100/0/threaded>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2008-06.html>
- * CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=2549
- * CONFIRM:
<http://wiki.rpath.com/Advisories:rPSA-2008-0336>
- * DEBIAN: DSA-1673
<http://www.debian.org/security/2008/dsa-1673>
- * MANDRIVA: MDVSA-2008:215
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:215>
- * BID: 31838
<http://www.securityfocus.com/bid/31838>
- * FRSIRT: ADV-2008-2872
<http://www.frsirt.com/english/advisories/2008/2872>
- * SECTrack: 1021069
<http://securitytracker.com/id?1021069>
- * SECUNIA: 32355
<http://secunia.com/advisories/32355>
- * SECUNIA: 32944
<http://secunia.com/advisories/32944>

CVE Reference:

CVE-2008-4684 (cve.mitre.org, nvd.nist.gov)

• 18275 Wireshark Bluetooth RFCOMM dissector denial of service Vulnerability (Remote File Checking)

Unspecified vulnerability in the Bluetooth RFCOMM dissector in Wireshark 0.99.7 through 1.0.3 allows remote attackers to cause a denial of service (application crash or abort) via unknown packets.

The vulnerability is reported in versions 0.99.7 to 1.0.3.

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

References:

- * BUGTRAQ: 20081211 rPSA-2008-0336-1 tshark wireshark
<http://www.securityfocus.com/archive/1/archive/1/499154/100/0/threaded>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2008-06.html>
- * CONFIRM:
<http://wiki.rpath.com/Advisories:rPSA-2008-0336>
- * MANDRIVA: MDVSA-2008:215
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:215>
- * BID: 31838
<http://www.securityfocus.com/bid/31838>
- * FRSIRT: ADV-2008-2872
<http://www.frsirt.com/english/advisories/2008/2872>
- * SECTRAK: 1021069
<http://securitytracker.com/id?1021069>
- * SECUNIA: 32355
<http://secunia.com/advisories/32355>
- * XF: wireshark-bluetoothrfcomm-dos(46014)
<http://xforce.iss.net/xforce/xfdb/46014>

CVE Reference:

CVE-2008-4681 (cve.mitre.org, nvd.nist.gov)

• 18276 Wireshark SMTP dissector denial of service Vulnerability (Remote File Checking)

Wireshark 1.0.4 and earlier allows remote attackers to cause a denial of service via a long SMTP request, which triggers an infinite loop.

The vulnerability is reported in version prior to 1.0.5.

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

References:

- * BUGTRAQ: 20081122 [SVRT-04-08] Vulnerability in WireShark 1.0.4 for DoS Attack
<http://www.securityfocus.com/archive/1/archive/1/498562/100/0/threaded>
- * BUGTRAQ: 20081211 rPSA-2008-0336-1 tshark wireshark
<http://www.securityfocus.com/archive/1/archive/1/499154/100/0/threaded>
- * FULLDISC: 20081122 [SVRT-04-08] Vulnerability in WireShark 1.0.4 for DoS Attack
<http://lists.grok.org.uk/pipermail/full-disclosure/2008-November/065840.html>
- * MLIST: [oss-security] 20081124 CVE Request -- wireshark
<http://www.openwall.com/lists/oss-security/2008/11/24/1>
- * CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=472737
- * CONFIRM:
<http://wiki.rpath.com/Advisories:rPSA-2008-0336>
- * FRSIRT: ADV-2008-3231
<http://www.frsirt.com/english/advisories/2008/3231>
- * SECTRAK: 1021275
<http://www.securitytracker.com/id?1021275>
- * SECUNIA: 32840
<http://secunia.com/advisories/32840>
- * SREASON: 4663
<http://securityreason.com/securityalert/4663>

CVE Reference:

CVE-2008-5285 (cve.mitre.org, nvd.nist.gov)

• 18277 Wireshark WLCCP dissector denial of service Vulnerability (Remote File Checking)

An error in the WLCCP dissector can be exploited to trigger the execution of an infinite loop via a specially crafted packet.

The vulnerability is reported in versions 0.99.7 to 1.0.4.

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

References:

- * MISC: wnpa-sec-2008-07
<http://www.wireshark.org/security/wnpa-sec-2008-07.html>
- * SECUNIA: 32840
<http://secunia.com/advisories/32840/>

CVE Reference:

• **18278 Wireshark denial of service Vulnerability (Remote File Checking)**

On non-Windows systems, Wireshark could crash if the HOME environment variable contained sprintf-style string formatting characters.

The vulnerability is reported in versions 0.99.8 to 1.0.5.

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

References:

- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-01.html>
- * CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=3150
- * BID: 33690
<http://www.securityfocus.com/bid/33690>
- * FRSIRT: ADV-2009-0370
<http://www.frsirt.com/english/advisories/2009/0370>

CVE Reference:

CVE-2009-0601 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2008-4285 IBM CVSS 2.0 Score = 5.0**

Unspecified vulnerability in the Performance Monitoring Infrastructure (PMI) feature in the Servlet Engine/Web Container component in IBM WebSphere Application Server (WAS) 6.1.x before 6.1.0.19, when a component statistic is enabled, allows attackers to cause a denial of service (daemon crash) via vectors related to "a gradual degradation in performance."

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

References:

- CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27007951>
- AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg24019260>
- XF: <http://xforce.iss.net/xforce/xfdb/48698>

CVE Reference: [CVE-2008-4285](http://cve.mitre.org/cve/2008/4285)

• **CVE-2009-0504 IBM CVSS 2.0 Score = 2.1**

WSPolicy in the Web Services component in IBM WebSphere Application Server (WAS) 7.0.x before 7.0.0.1 does not properly recognize the IDAssertion.isUsed binding property, which allows local users to discover a password by reading a SOAP message.

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

References:

- CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27014463>
- XF: <http://xforce.iss.net/xforce/xfdb/48700>
- AIXAPAR: <http://www-1.ibm.com/support/docview.wss?uid=swg1PK73573>

CVE Reference: [CVE-2009-0504](http://cve.mitre.org/cve/2009/0504)

• **CVE-2009-0310 Novell CVSS 2.0 Score = 10.0**

Buffer overflow in SUSE blinux (aka sbl) in SUSE openSUSE 10.3 through 11.0 has unknown impact and attack vectors related to "incoming data and authentication-strings."

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

References:

BID: <http://www.securityfocus.com/bid/33794>

SUSE: <http://lists.opensuse.org/opensuse-security-announce/2009-02/msg00002.html>

CVE Reference: [CVE-2009-0310](#)

• **CVE-2009-0609 Sun CVSS 2.0 Score = 7.8**

Sun Java System Directory Proxy Server in Sun Java System Directory Server Enterprise Edition 6.0 through 6.3, when a JDBC data source is used, does not properly handle (1) a long value in an ADD or (2) long string attributes, which allows remote attackers to cause a denial of service (JDBC backend outage) via crafted LDAP requests.

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

References:

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-66-251086-1>

CONFIRM: <http://sunsolve.sun.com/search/document.do?assetkey=1-21-125276-08-1>

BID: <http://www.securityfocus.com/bid/33761>

SECUNIA: <http://secunia.com/advisories/33923>

CVE Reference: [CVE-2009-0609](#)

• **CVE-2009-0605 Linux CVSS 2.0 Score = 4.9**

Stack consumption vulnerability in the do_page_fault function in arch/x86/mm/fault.c in the Linux kernel before 2.6.28.5 allows local users to cause a denial of service (memory corruption) or possibly gain privileges via unspecified vectors that trigger page faults on a machine that has a registered Kprobes probe.

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

References:

BID: <http://www.securityfocus.com/bid/33758>

CONFIRM: <http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.28.5>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/stable/linux-2.6.27.y.git;a=commit;h=9be260a646bf76fa418ee519afa10196b316468>

CVE Reference: [CVE-2009-0605](#)

• **CVE-2009-0611 Novell CVSS 2.0 Score = 4.3**

Multiple cross-site scripting (XSS) vulnerabilities in qfsearch/AdminServlet in QuickFinder Server in Novell Open Enterprise Server 1.x allow remote attackers to inject arbitrary web script or HTML via (1) the siteloc parameter in a displayaddsite action, the site parameter in a (2) generalproperties or (3) clusterserviceproperties action, (4) the adminurl parameter in a global action, or (5) the print-list parameter.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/48619>

SECTRACK: <http://www.securitytracker.com/id?1021695>

BID: <http://www.securityfocus.com/bid/33708>

SECUNIA: <http://secunia.com/advisories/33886>

MISC: <http://packetstormsecurity.org/0902-exploits/nqfs-xss.txt>

CVE Reference: [CVE-2009-0611](#)

• **CVE-2009-0599 Wireshark CVSS 2.0 Score = 5.0**

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.

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

References:

BID: <http://www.securityfocus.com/bid/33690>

FRSIRT: <http://www.frsirt.com/english/advisories/2009/0370>

CONFIRM: <https://bugs.wireshark.org/bugzilla/attachment.cgi?id=2590>

CONFIRM: <http://www.wireshark.org/security/wnpa-sec-2009-01.html>

SECUNIA: <http://secunia.com/advisories/33872>

OSVDB: <http://osvdb.org/51815>

CVE Reference: [CVE-2009-0599](https://cve.mitre.org/cve/2009/0599)

• **CVE-2009-0600 Wireshark CVSS 2.0 Score = 4.3**

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.

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

References:

FRSIRT: <http://www.frsirt.com/english/advisories/2009/0370>

CONFIRM: https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=1937

CONFIRM: <http://www.wireshark.org/security/wnpa-sec-2009-01.html>

BID: <http://www.securityfocus.com/bid/33690>

SECUNIA: <http://secunia.com/advisories/33872>

CVE Reference: [CVE-2009-0600](https://cve.mitre.org/cve/2009/0600)

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