

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

The eternal race. IOS browser problem may be more serious. Hackers targeting PR bureaus. NSA director on threads.

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

• The Changing Threat Landscape

CSO - In covering the security threat landscape over the years, two fundamental issues have stayed constant. First, the threat landscape continues to evolve and gain sophistication. Second, attackers will always be a step ahead of the defenders in exploiting vulnerabilities across the spectrum of people, process and technologies. But what's different today is the motivation, methods and tools of these attacks: we're no longer fighting an individual hacker, but a highly organized, well-funded crime syndicate, and in some cases, even a state sponsored agent.

Also see Kark's Building a business case for information security

As IT security professionals work toward building their high-performance security organization, it will be essential to consider the changing nature of the threat landscape. In particular: Computerworld

Full Story :

http://www.computerworld.com/s/article/9180262/The_Changing_Threat_Landscape?source=rss_security

• Experts devise theoretical attacks with iOS browser security hole

The new browser security flaw in iPhones, iPods, and iPads could be more dangerous than initially suspected.

The vulnerability comes from the way the jailbreak software, released on Sunday, uses the mobile Safari browser instead of requiring that the device be connected to a computer. Jailbreaking the phone allows it to run apps not approved by Apple. But this flaw could be used to launch an exploit if the user were to surf to a Web site hosting a malicious PDF, giving unrestricted access to the device.

"The same PDF exploit used to jailbreak the device could also be used to install something malicious," security expert Mike Kershaw told CNET on Thursday. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20012860-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• Hackers find a new target in payroll processing

IDG News Service - Depression-era bank robber Slick Willie Sutton is famous for saying that he robbed banks "because that's where the money is." If he were around today, he'd have other options.

In what may be a troubling sign of things to come, criminals recently hacked into a desktop computer belonging to Regeneron Pharmaceuticals and tried to steal money by redirecting funds using Regeneron's account on the company's third-party payroll system, operated by Ceridian.

The attack didn't work, but it shows that criminals, who have been making millions of dollars by hacking into computers and initiating fraudulent bank transfers, may have found a new target. Computerworld

Full Story :

http://www.computerworld.com/s/article/9180220/Hackers_find_a_new_target_in_payroll_processing?source=rss_se

• Cyber Command chief details threats to U.S.

If the United States wants to defend itself against cyberattacks, it needs to focus on four key areas, according to United States Cyber Command head and NSA Director Army Gen. Keith Alexander.

U.S. CyberCom head General Keith Alexander

(Credit: National Security Agency) Cnet Security

Full Story :

http://news.cnet.com/8301-13639_3-20012774-42.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 18863 Wireshark SigComp Universal Decompressor Virtual Machine denial of service Vulnerability (Remote File Checking)

The SigComp Universal Decompressor Virtual Machine dissector in Wireshark 0.10.7 through 1.0.13 and 1.2.0 through 1.2.8 allows remote attackers to cause a denial of service (infinite loop) via unknown vectors.

The vulnerability is reported in versions 0.10.7 up to and including 1.0.13, 1.2.0 up to and including 1.2.8.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Crash / 100% CPU** Risk: **High**

References:

* MLIST: [oss-security] 20100610 CVE request for new wireshark vulnerabilities

<http://www.openwall.com/lists/oss-security/2010/06/11/1>

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2010-05.html>

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2010-06.html>

* MANDRIVA: MDVSA-2010:113

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:113>

* BID: 40728

<http://www.securityfocus.com/bid/40728>

* SECUNIA: 40112

<http://secunia.com/advisories/40112>

* VUPEN: ADV-2010-1418

<http://www.vupen.com/english/advisories/2010/1418>

CVE Reference:

CVE-2010-2286 (cve.mitre.org, nvd.nist.gov)

• **18864 Wireshark SigComp Universal Decompressor Virtual Machine buffer overflow Vulnerability (Remote File Checking)**

Buffer overflow in the SigComp Universal Decompressor Virtual Machine dissector in Wireshark 0.10.8 through 1.0.13 and 1.2.0 through 1.2.8 has unknown impact and remote attack vectors.

The vulnerability is reported in versions 0.10.8 up to and including 1.0.13, 1.2.0 up to and including 1.2.8.

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

References:

- * MLIST: [oss-security] 20100610 CVE request for new wireshark vulnerabilities
<http://www.openwall.com/lists/oss-security/2010/06/11/1>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2010-05.html>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2010-06.html>
- * MANDRIVA: MDVSA-2010:113
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:113>
- * BID: 40728
<http://www.securityfocus.com/bid/40728>
- * SECUNIA: 40112
<http://secunia.com/advisories/40112>
- * VUPEN: ADV-2010-1418
<http://www.vupen.com/english/advisories/2010/1418>

CVE Reference:

CVE-2010-2287 (cve.mitre.org, nvd.nist.gov)

• **18865 Shortcut Icon Loading Vulnerability (MS10-046/2286198) (Remote File Checking)**

A remote code execution vulnerability exists in affected versions of Microsoft Windows. The vulnerability exists because Windows incorrectly parses shortcuts in such a way that malicious code may be executed when the operating system displays the icon of a malicious shortcut file. An attacker who successfully exploited this vulnerability could run arbitrary code as the logged-on user. This update addresses a vulnerability previously discussed in Microsoft Security Advisory 2286198.

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

References:

- * MISC:
<http://isc.sans.edu/diary.html?storyid=9181>
- * MISC:
<http://isc.sans.edu/diary.html?storyid=9190>
- * MISC:
<http://krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw/>
- * MISC:
<http://www.f-secure.com/weblog/archives/00001986.html>
- * MISC:
http://www.f-secure.com/weblog/archives/new_rootkit_en.pdf
- * CONFIRM:
<http://www.microsoft.com/technet/security/advisory/2286198.mspx>
- * CERT-VN: VU#940193
<http://www.kb.cert.org/vuls/id/940193>
- * BID: 41732
<http://www.securityfocus.com/bid/41732>
- * SECTRAK: 1024216
<http://securitytracker.com/id?1024216>
- * SECUNIA: 40647
<http://secunia.com/advisories/40647>
- * MS: MS10-046
<http://www.microsoft.com/technet/security/bulletin/MS10-046.mspx>

CVE Reference:

CVE-2010-2568 (cve.mitre.org, nvd.nist.gov)

• **18866 Apache mod_proxy_ajp Denial of Service Vulnerability**

mod_proxy_ajp would return the wrong status code if it encountered an error, causing a backend server to be put into an error state until the retry timeout expired. A remote attacker could send malicious requests to trigger this issue, resulting in denial of service.

The issue is fixed in version 2.2.15.

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

References:

* CONFIRM:

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

* CONFIRM:

http://svn.apache.org/viewvc/httpd/httpd/branches/2.2.x/modules/proxy/mod_proxy_ajp.c?r1=917876&r2=917875&

* CONFIRM:

<http://svn.apache.org/viewvc?view=revision&revision=917876>

* CONFIRM:

https://bugzilla.redhat.com/show_bug.cgi?id=569905

* AIXAPAR: PM12247

<http://www-01.ibm.com/support/docview.wss?uid=swg1PM12247>

* AIXAPAR: PM08939

<http://www-01.ibm.com/support/docview.wss?uid=swg1PM08939>

* AIXAPAR: PM15829

<http://www-01.ibm.com/support/docview.wss?uid=swg1PM15829>

* DEBIAN: DSA-2035

<http://www.debian.org/security/2010/dsa-2035>

* FEDORA: FEDORA-2010-5942

<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/039957.html>

* FEDORA: FEDORA-2010-6131

<http://lists.fedoraproject.org/pipermail/package-announce/2010-May/040652.html>

* MANDRIVA: MDVSA-2010:053

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:053>

* REDHAT: RHSA-2010:0168

<http://www.redhat.com/support/errata/RHSA-2010-0168.html>

* SUSE: SUSE-SR:2010:010

<http://lists.opensuse.org/opensuse-security-announce/2010-04/msg00006.html>

* BID: 38491

<http://www.securityfocus.com/bid/38491>

* SECUNIA: 39628

<http://secunia.com/advisories/39628>

* SECUNIA: 39632

<http://secunia.com/advisories/39632>

* SECUNIA: 39656

<http://secunia.com/advisories/39656>

* SECUNIA: 39501

<http://secunia.com/advisories/39501>

* SECUNIA: 40096

<http://secunia.com/advisories/40096>

* SECUNIA: 39100

<http://secunia.com/advisories/39100>

* VUPEN: ADV-2010-0994

<http://www.vupen.com/english/advisories/2010/0994>

* VUPEN: ADV-2010-1001

<http://www.vupen.com/english/advisories/2010/1001>

* VUPEN: ADV-2010-1057

<http://www.vupen.com/english/advisories/2010/1057>

* VUPEN: ADV-2010-0911

<http://www.vupen.com/english/advisories/2010/0911>

* VUPEN: ADV-2010-1411

<http://www.vupen.com/english/advisories/2010/1411>

CVE Reference:

CVE-2010-0408 (cve.mitre.org, nvd.nist.gov)

• 18867 Apache Subrequest handling of request headers Vulnerability

A flaw in the core subrequest process code was fixed, to always provide a shallow copy of the headers_in array to the subrequest, instead of a pointer to the parent request's array as it had for requests without request bodies. This meant all modules such as mod_headers which may manipulate the input headers for a subrequest would poison the parent request in two ways, one by modifying the parent request, which might not be intended, and second by leaving

pointers to modified header fields in memory allocated to the subrequest scope, which could be freed before the main request processing was finished, resulting in a segfault or in revealing data from another request on threaded servers, such as the worker or winnt MPMs.

The issue is fixed in versions 2.0.64, and 2.2.15.

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

References:

* CONFIRM:

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

* CONFIRM:

<http://svn.apache.org/viewvc/httpd/httpd/branches/2.2.x/server/protocol.c?r1=917617&r2=917867&pathrev=917867>

* CONFIRM:

<http://svn.apache.org/viewvc?view=revision&revision=917867>

* CONFIRM:

<http://svn.apache.org/viewvc?view=revision&revision=918427>

* CONFIRM:

https://bugzilla.redhat.com/show_bug.cgi?id=570171

* CONFIRM:

https://issues.apache.org/bugzilla/show_bug.cgi?id=48359

* AIXAPAR: PM12247

<http://www-01.ibm.com/support/docview.wss?uid=swg1PM12247>

* AIXAPAR: PM08939

<http://www-01.ibm.com/support/docview.wss?uid=swg1PM08939>

* AIXAPAR: PM15829

<http://www-01.ibm.com/support/docview.wss?uid=swg1PM15829>

* DEBIAN: DSA-2035

<http://www.debian.org/security/2010/dsa-2035>

* FEDORA: FEDORA-2010-5942

<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/039957.html>

* FEDORA: FEDORA-2010-6131

<http://lists.fedoraproject.org/pipermail/package-announce/2010-May/040652.html>

* REDHAT: RHSA-2010:0168

<http://www.redhat.com/support/errata/RHSA-2010-0168.html>

* REDHAT: RHSA-2010:0175

<http://www.redhat.com/support/errata/RHSA-2010-0175.html>

* SUSE: SUSE-SR:2010:010

<http://lists.opensuse.org/opensuse-security-announce/2010-04/msg00006.html>

* BID: 38494

<http://www.securityfocus.com/bid/38494>

* SECUNIA: 39628

<http://secunia.com/advisories/39628>

* SECUNIA: 39632

<http://secunia.com/advisories/39632>

* SECUNIA: 39656

<http://secunia.com/advisories/39656>

* SECUNIA: 39501

<http://secunia.com/advisories/39501>

* SECUNIA: 40096

<http://secunia.com/advisories/40096>

* SECUNIA: 39100

<http://secunia.com/advisories/39100>

* SECUNIA: 39115

<http://secunia.com/advisories/39115>

* VUPEN: ADV-2010-0994

<http://www.vupen.com/english/advisories/2010/0994>

* VUPEN: ADV-2010-1001

<http://www.vupen.com/english/advisories/2010/1001>

* VUPEN: ADV-2010-1057

<http://www.vupen.com/english/advisories/2010/1057>

* VUPEN: ADV-2010-0911

<http://www.vupen.com/english/advisories/2010/0911>

* VUPEN: ADV-2010-1411

<http://www.vupen.com/english/advisories/2010/1411>

* XF: apache-http-rh-info-disclosure(56625)

<http://xforce.iss.net/xforce/xfdb/56625>

CVE Reference:

CVE-2010-0434 (cve.mitre.org, nvd.nist.gov)

• 18868 Apache mod_isapi module Denial of Service Vulnerability

A flaw was found with within mod_isapi which would attempt to unload the ISAPI dll when it encountered various error states. This could leave the callbacks in an undefined state and result in a segfault. On Windows platforms using mod_isapi, a remote attacker could send a malicious request to trigger this issue, and as win32 MPM runs only one process, this would result in a denial of service, and potentially allow arbitrary code execution.

The issue is fixed in versions 2.0.64, and 2.2.15.

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

References:

* MISC:

<http://www.senseofsecurity.com.au/advisories/SOS-10-002>

* CONFIRM:

<http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=917870&r2=917869&pathrev=917870>

* CONFIRM:

http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/arch/win32/mod_isapi.c?r1=917870&r2=917869&pathrev=917870

* CONFIRM:

<http://svn.apache.org/viewvc?view=revision&revision=917870>

* CONFIRM:

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

* CONFIRM:

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

* AIXAPAR: PM09447

<http://www-01.ibm.com/support/docview.wss?uid=swg1PM09447>

* AIXAPAR: PM12247

<http://www-01.ibm.com/support/docview.wss?uid=swg1PM12247>

* CERT-VN: VU#280613

<http://www.kb.cert.org/vuls/id/280613>

* BID: 38494

<http://www.securityfocus.com/bid/38494>

* SECTRAK: 1023701

<http://www.securitytracker.com/id?1023701>

* SECUNIA: 38978

<http://secunia.com/advisories/38978>

* SECUNIA: 39628

<http://secunia.com/advisories/39628>

* VUPEN: ADV-2010-0634

<http://www.vupen.com/english/advisories/2010/0634>

* VUPEN: ADV-2010-0994

<http://www.vupen.com/english/advisories/2010/0994>

* XF: apache-http-modisapi-ocp-unspecified(56624)

<http://xforce.iss.net/xforce/xfdb/56624>

CVE Reference:

CVE-2010-0425 (cve.mitre.org, nvd.nist.gov)

• 18869 Apache mod_cache and mod_dav Denial of Service Vulnerabilities

A flaw was found in the handling of requests by mod_cache and mod_dav. A malicious remote attacker could send a carefully crafted request and cause a httpd child process to crash. This crash would only be a denial of service if using the worker MPM. This issue is further mitigated as mod_dav is only affected by requests that are most likely to be authenticated, and mod_cache is only affected if the uncommon "CacheIgnoreURLSessionIdentifiers" directive, introduced in version 2.2.14, is used.

The issue is fixed in version 2.2.16.

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

References:

* MLIST: [apache-announce] 20100725 [ANNOUNCEMENT] Apache HTTP Server 2.2.16 Released

<http://marc.info/?l=apache-announce&m=128009718610929&w=2>

* CONFIRM:

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

* CONFIRM:

https://issues.apache.org/bugzilla/show_bug.cgi?id=49246

CVE Reference:

CVE-2010-1452 (cve.mitre.org, nvd.nist.gov)

• 18870 Apache mod_proxy_http information disclosure Vulnerability

An information disclosure flaw was found in mod_proxy_http in versions 2.2.9 through 2.2.15, 2.3.4-alpha and 2.3.5-alpha. Under certain timeout conditions, the server could return a response intended for another user. Only Windows, Netware and OS2 operating systems are affected. Only those configurations which trigger the use of proxy worker pools are affected. There was no vulnerability on earlier versions, as proxy pools were not yet introduced.

The issue is fixed in version 2.2.16.

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

References:

- * BUGTRAQ: 20100611 [advisory] httpd Timeout detection flaw (mod_proxy_http) CVE-2010-2068
<http://www.securityfocus.com/archive/1/archive/1/511809/100/0/threaded>
- * MLIST: [httpd-announce] 20100611 [advisory] httpd Timeout detection flaw (mod_proxy_http) CVE-2010-2068
http://mail-archives.apache.org/mod_mbox/httpd-announce/201006.mbox/%3C4C12933D.4060400@apache.org%3E
- * MLIST: [apache-announce] 20100725 [ANNOUNCEMENT] Apache HTTP Server 2.2.16 Released
<http://marc.info/?l=apache-announce&m=128009718610929&w=2>
- * CONFIRM:
http://httpd.apache.org/security/vulnerabilities_22.html
- * CONFIRM:
http://www.apache.org/dist/httpd/patches/apply_to_2.2.15/CVE-2010-2068-r953616.patch
- * CONFIRM:
http://www.apache.org/dist/httpd/patches/apply_to_2.3.5/CVE-2010-2068-r953418.patch
- * BID: 40827
<http://www.securityfocus.com/bid/40827>
- * SECTRAK: 1024096
<http://securitytracker.com/id?1024096>
- * SECUNIA: 40206
<http://secunia.com/advisories/40206>
- * VUPEN: ADV-2010-1436
<http://www.vupen.com/english/advisories/2010/1436>
- * XF: apache-modproxyhttp-timeout-info-disc(59413)
<http://xforce.iss.net/xforce/xfdb/59413>

CVE Reference:

CVE-2010-2068 (cve.mitre.org, nvd.nist.gov)

• 18871 Apache mod_proxy overflow Vulnerability

An incorrect conversion between numeric types flaw was found in the mod_proxy module which affects some 64-bit architecture systems. A malicious HTTP server to which requests are being proxied could use this flaw to trigger a heap buffer overflow in an httpd child process via a carefully crafted response.

The issue is fixed in version 1.3.42.

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

References:

- * BUGTRAQ: 20100127 Mod_proxy from apache 1.3 - Integer overflow which causes heap overflow.
<http://www.securityfocus.com/archive/1/archive/1/509185/100/0/threaded>
- * FULLDISC: 20100127 Mod_proxy from apache 1.3 - Integer overflow which causes heap overflow.
<http://archives.neohapsis.com/archives/fulldisclosure/2010-01/0589.html>
- * MISC:
<http://blog.pi3.com.pl/?p=69>
- * MISC:
<http://packetstormsecurity.org/1001-exploits/modproxy-overflow.txt>
- * MISC:
http://site.pi3.com.pl/adv/mod_proxy.txt
- * SUSE: SUSE-SR:2010:010
<http://lists.opensuse.org/opensuse-security-announce/2010-04/msg00006.html>
- * BID: 37966
<http://www.securityfocus.com/bid/37966>
- * SECTRAK: 1023533
<http://www.securitytracker.com/id?1023533>
- * SECUNIA: 38319

<http://secunia.com/advisories/38319>

* SECUNIA: 39656

<http://secunia.com/advisories/39656>

* VUPEN: ADV-2010-0240

<http://www.vupen.com/english/advisories/2010/0240>

* VUPEN: ADV-2010-1001

<http://www.vupen.com/english/advisories/2010/1001>

* XF: modproxy-approxysendfb-bo(55941)

<http://xforce.iss.net/xforce/xfdb/55941>

CVE Reference:

CVE-2010-0010 (cve.mitre.org, nvd.nist.gov)

• 18872 Apache Tomcat authentication headers Information disclosure Vulnerability

Apache Tomcat is a freely available, open source application server maintained by the Apache Foundation.

The WWW-Authenticate HTTP header for BASIC and DIGEST authentication includes a realm name. If a <realm-name> element is specified for the application in web.xml it will be used. However, a <realm-name> is not specified then Tomcat will generate realm name using the code snippet request.getServerName() + ":" + request.getServerPort(). In some circumstances this can expose the local host name or IP address of the machine running Tomcat.

The issue has been addressed in Apache Tomcat version 6.0.26, 5.5.30.

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

References:

* BUGTRAQ: 20100421 [SECURITY] CVE-2010-1157: Apache Tomcat information disclosure vulnerability

<http://www.securityfocus.com/archive/1/archive/1/510879/100/0/threaded>

* CONFIRM:

<http://tomcat.apache.org/security-5.html>

* CONFIRM:

<http://tomcat.apache.org/security-6.html>

* CONFIRM:

<http://svn.apache.org/viewvc?view=revision&revision=936540>

* CONFIRM:

<http://svn.apache.org/viewvc?view=revision&revision=936541>

* BID: 39635

<http://www.securityfocus.com/bid/39635>

* SECUNIA: 39574

<http://secunia.com/advisories/39574>

* VUPEN: ADV-2010-0980

<http://www.vupen.com/english/advisories/2010/0980>

CVE Reference:

CVE-2010-1157 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-2927 IBM CVSS 2.0 Score = 5.0

The slapi_printmessage function in IBM Tivoli Directory Server (ITDS) before 6.0.0.8-TIV-ITDS-IF0006 allows remote attackers to cause a denial of service (daemon crash) via multiple incomplete DIGEST-MD5 connection attempts.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg24027463>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1IO12399>

BID: <http://www.securityfocus.com/bid/42093>

SECUNIA: <http://secunia.com/advisories/40791>

CVE Reference: [CVE-2010-2927](http://cve.mitre.org)

• **CVE-2010-1794 Apple CVSS 2.0 Score = 4.9**

The webdav_mount function in webdav_vfsops.c in the WebDAV kernel extension (aka webdav_fs.kext) for Mac OS X 10.6 allows local users to cause a denial of service (panic) via a mount request with a large integer in the pa_socket_namelen field.

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

References:

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/512642/100/0/threaded>

BID: <http://www.securityfocus.com/bid/41958>

SECTRAK: <http://securitytracker.com/id?1024250>

CVE Reference: [CVE-2010-1794](#)

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