

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

Advice on the most critical security holes. Wikileaks supporters arrested. Another go at California data breach bill. The hackers get hacked.

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

• Six security leaks to plug right now

Computerworld - Just as the Titanic was thought to be unsinkable, many of today's enterprises think of themselves as invulnerable. Yet, for every large organization that glides through the year without any mishaps, there are many others that suffer break-ins, Wi-Fi sniffing snafus and incidents where Bluetooth "sniper rifles" are used to steal company secrets.

Security consultants have identified six holes that are often wide open in corporate IT systems, even at companies that take great pride in their security precautions.

1. Unauthorized Smartphones on Wi-Fi Networks Smartphones create some of the greatest risks for enterprise security, mostly because they're so common and because some employees just can't resist using personal devices in the office -- even if their employers have well-established policies prohibiting their use. Computerworld

Full Story :

http://www.computerworld.com/s/article/353317/Six_Leaks_to_Plug_Right_Now?source=rss_security

• Five charged with "Anonymous"-led DDoS attacks

London police on Thursday charged two boys and three men for their role in launching distributed denial-of-service (DDoS) attacks against commercial websites.

The males, ages 15, 16, 19, 20 and 26, were arrested at their homes during early-morning raids and were charged under the Computer Misuse Act, according to a news release. They were brought to local police stations for processing.

Authorities believe the suspects are connected to the Anonymous hacking group, a loosely affiliated band of web savvy, politically motivated individuals. The hacktivist gang is being investigated for its role in taking down a number of high-profile websites, including Visa and PayPal, after those companies decided to cut ties with WikiLeaks following the whistleblower site's disclosure of thousands of U.S. diplomatic cables. SC Magazine

Full Story :

http://www.scmagazineus.com/five-charged-with-anonymous-led-ddos-attacks/article/195124/?utm_source=feedburn

• California lawmaker tries again with data breach bill

For a third time, a California lawmaker has introduced a bill that would update the state's pioneering data breach notification law, SB-1386, to include additional requirements for organizations that lose sensitive data.

The proposal, introduced Thursday by Democratic state Sen. Joe Simitian, would require that breach notification letters contain specifics of the incident, including the type of personal information exposed, a description of what happened, and advice on steps to take to protect oneself from identity theft. The law also would mandate that organizations that suffer a breach affecting 500 or more people must submit a copy of the alert letter to the state attorney general's office.

Twice before, the bill has gone to former Gov. Arnold Schwarzenegger's desk to be signed but was vetoed. SC Magazine

Full Story :

http://www.scmagazineus.com/california-lawmaker-tries-again-with-data-breach-bill/article/194988/?utm_source=feedburn

• Site of AT&T-iPad hackers is hacked

The Web site of the hacker group whose members were charged with computer crimes after they exposed a hole in AT&T's site for iPad customers last year was hacked today.

For at least a few hours an obscenity-laden message on the Goatse Security site said: "I have taken the liberty of exposing your gaping hole...As you are a group of self-aggrandizing [profanity redacted], I have also contacted the media to ensure that this incident gets the coverage it deserves.

"In cracking this site, I have sent specially crafted requests to the server with my browser ID spoofed to that of an iPad. Please know that while this was not instrumental in this wondrous crack, it WAS poetic in many ways. I also gave Goatsec the same warning that they gave AT&T... none at all, to patch their gaping hole. User Accounts have been deleted, and passwords changed," the note said. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20029734-245.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 19165 PHP `html_entity_decode()` Interruption Information Leak Vulnerability

The `html_entity_decode` function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal call, related to the call time pass by reference feature.

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

References:

* MISC:

http://php-security.org/2010/05/06/mops-2010-010-php-html_entity_decode-interruption-information-leak-vulnerability/index.html

* SUSE: SUSE-SR:2010:017

<http://lists.opensuse.org/opensuse-security-announce/2010-09/msg00006.html>

* SUSE: SUSE-SR:2010:018

<http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00000.html>

CVE Reference:

CVE-2010-1860 (cve.mitre.org, nvd.nist.gov)

• 19166 PHP chunk_split() Interruption Information Leak Vulnerability

The chunk_split function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

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

References:

* MISC:

http://php-security.org/2010/05/04/mops-2010-008-php-chunk_split-interruption-information-leak-vulnerability/index.html

* SUSE: SUSE-SR:2010:017

<http://lists.opensuse.org/opensuse-security-announce/2010-09/msg00006.html>

* SUSE: SUSE-SR:2010:018

<http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00000.html>

CVE Reference:

CVE-2010-1862 (cve.mitre.org, nvd.nist.gov)

• 19167 PHP addcslashes() Interruption Information Leak Vulnerability

The addcslashes function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

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

References:

* MISC:

<http://php-security.org/2010/05/03/mops-2010-006-php-addcslashes-interruption-information-leak-vulnerability/index.html>

* SUSE: SUSE-SR:2010:017

<http://lists.opensuse.org/opensuse-security-announce/2010-09/msg00006.html>

* SUSE: SUSE-SR:2010:018

<http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00000.html>

CVE Reference:

CVE-2010-1864 (cve.mitre.org, nvd.nist.gov)

• 19168 PHP iconv_mime_encode(), conv_mime_decode, and iconv_substr Interruption Information Leak Vulnerability

The (1) iconv_mime_decode, (2) iconv_substr, and (3) iconv_mime_encode functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

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

References:

* MISC:

http://php-security.org/2010/05/18/mops-2010-032-php-iconv_mime_decode-interruption-information-leak-vulnerability/index.html

* MISC:

http://php-security.org/2010/05/18/mops-2010-033-php-iconv_substr-interruption-information-leak-vulnerability/index.html

* MISC:

http://php-security.org/2010/05/18/mops-2010-034-php-iconv_mime_encode-interruption-information-leak-vulnerability/index.html

* SUSE: SUSE-SR:2010:017

<http://lists.opensuse.org/opensuse-security-announce/2010-09/msg00006.html>

* SUSE: SUSE-SR:2010:018

<http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00000.html>

CVE Reference:

CVE-2010-2097 (cve.mitre.org, nvd.nist.gov)

• 19169 PHP htmlentities, htmlspecialchars, str_getcsv, http_build_query, strpbrk, and strstr functions Information Leak Vulnerability

The (1) htmlentities, (2) htmlspecialchars, (3) str_getcsv, (4) http_build_query, (5) strpbrk, and (6) strstr functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

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

References:

* MISC:

<http://php-security.org/2010/05/21/mops-2010-036-php-htmlentities-and-htmlspecialchars-interruption-information-leak-vul>

* MISC:

http://php-security.org/2010/05/21/mops-2010-037-php-str_getcsv-interruption-information-leak-vulnerability/index.html

* MISC:

http://php-security.org/2010/05/21/mops-2010-038-php-http_build_query-interruption-information-leak-vulnerability/index.html

* MISC:

<http://php-security.org/2010/05/21/mops-2010-039-php-strpbrk-interruption-information-leak-vulnerability/index.html>

* MISC:

<http://php-security.org/2010/05/21/mops-2010-040-php-strstr-interruption-information-leak-vulnerability/index.html>

* SUSE: SUSE-SR:2010:017

<http://lists.opensuse.org/opensuse-security-announce/2010-09/msg00006.html>

* SUSE: SUSE-SR:2010:018

<http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00000.html>

CVE Reference:

CVE-2010-2100 (cve.mitre.org, nvd.nist.gov)

• 19170 PHP strip_tags, setcookie, strtok, wordwrap, str_word_count, and str_pad functions Information Leak Vulnerability

The (1) strip_tags, (2) setcookie, (3) strtok, (4) wordwrap, (5) str_word_count, and (6) str_pad functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

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

References:

* MISC:

http://php-security.org/2010/05/26/mops-2010-041-php-strip_tags-interruption-information-leak-vulnerability/index.html

* MISC:

<http://php-security.org/2010/05/26/mops-2010-042-php-setcookie-interruption-information-leak-vulnerability/index.html>

* MISC:

<http://php-security.org/2010/05/26/mops-2010-043-php-strtok-interruption-information-leak-vulnerability/index.html>

* MISC:

<http://php-security.org/2010/05/26/mops-2010-044-php-wordwrap-interruption-information-leak-vulnerability/index.html>

* MISC:

http://php-security.org/2010/05/26/mops-2010-045-php-str_word_count-interruption-information-leak-vulnerability/index.html

* MISC:

http://php-security.org/2010/05/26/mops-2010-046-php-str_pad-interruption-information-leak-vulnerability/index.html

* SUSE: SUSE-SR:2010:017

<http://lists.opensuse.org/opensuse-security-announce/2010-09/msg00006.html>

* SUSE: SUSE-SR:2010:018

<http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00000.html>

CVE Reference:

CVE-2010-2101 (cve.mitre.org, nvd.nist.gov)

• 19171 PHP trim, ltrim, rtrim, and substr_replace functions Information Leak Vulnerability

The (1) trim, (2) ltrim, (3) rtrim, and (4) substr_replace functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

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

References:

* MISC:

<http://www.php-security.org/2010/05/30/mops-2010-047-php-trimltrimrtrim-interruption-information-leak-vulnerability/index.html>

* MISC:

http://www.php-security.org/2010/05/30/mops-2010-048-php-substr_replace-interruption-information-leak-vulnerability/index.html

- * SUSE: SUSE-SR:2010:017
<http://lists.opensuse.org/opensuse-security-announce/2010-09/msg00006.html>
- * SUSE: SUSE-SR:2010:018
<http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00000.html>
- * XF: php-substrreplace-info-disclosure(59220)
<http://xforce.iss.net/xforce/xfdb/59220>

CVE Reference:

CVE-2010-2190 (cve.mitre.org, nvd.nist.gov)

● 19172 Multiple PHP functions Information Leak Vulnerability

The (1) parse_str, (2) preg_match, (3) unpack, and (4) pack functions; the (5) ZEND_FETCH_RW, (6) ZEND_CONCAT, and (7) ZEND_ASSIGN_CONCAT opcodes; and the (8) ArrayObject::uasort method in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler. NOTE: vectors 2 through 4 are related to the call time pass by reference feature.

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

References:

- * MISC:
http://www.php-security.org/2010/05/31/mops-2010-049-php-parse_str-interruption-memory-corruption-vulnerability/index.html
- * MISC:
http://www.php-security.org/2010/05/31/mops-2010-050-php-preg_match-interruption-information-leak-vulnerability/index.html
- * MISC:
<http://www.php-security.org/2010/05/31/mops-2010-051-php-unpack-interruption-information-leak-vulnerability/index.html>
- * MISC:
<http://www.php-security.org/2010/05/31/mops-2010-052-php-pack-interruption-information-leak-vulnerability/index.html>
- * MISC:
http://www.php-security.org/2010/05/31/mops-2010-053-php-zend_fetch_rw-opcode-interruption-information-leak-vulnerability/index.html
- * MISC:
http://www.php-security.org/2010/05/31/mops-2010-054-php-zend_concatzend_assign_concat-opcode-interruption-information-leak-vulnerability/index.html
- * MISC:
<http://www.php-security.org/2010/05/31/mops-2010-055-php-arrayobjectuasort-interruption-memory-corruption-vulnerability/index.html>
- * SUSE: SUSE-SR:2010:017
<http://lists.opensuse.org/opensuse-security-announce/2010-09/msg00006.html>
- * SUSE: SUSE-SR:2010:018
<http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00000.html>
- * XF: php-parsestr-info-disclosure(59221)
<http://xforce.iss.net/xforce/xfdb/59221>

CVE Reference:

CVE-2010-2191 (cve.mitre.org, nvd.nist.gov)

● 19175 PHP 'php/ext/xml/xml.c' Integer Overflow Vulnerability

Integer overflow in the xml_utf8_decode function in ext/xml/xml.c in PHP before 5.2.11 makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string that uses overlong UTF-8 encoding, a different vulnerability than CVE-2010-3870.

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

References:

- * MISC:
<http://sirdarckcat.blogspot.com/2009/10/couple-of-unicode-issues-on-php-and.html>
- * MISC:
<http://www.blackhat.com/presentations/bh-usa-09/VELANAVA/BHUSA09-VelaNava-FavoriteXSS-SLIDES.pdf>
- * CONFIRM:
<http://bugs.php.net/bug.php?id=49687>
- * FEDORA: FEDORA-2010-18976
<http://lists.fedoraproject.org/pipermail/package-announce/2011-January/052845.html>
- * FEDORA: FEDORA-2010-19011
<http://lists.fedoraproject.org/pipermail/package-announce/2011-January/052836.html>
- * REDHAT: RHSA-2010:0919
<http://www.redhat.com/support/errata/RHSA-2010-0919.html>
- * UBUNTU: USN-1042-1
<http://www.ubuntu.com/usn/USN-1042-1>
- * BID: 44889

<http://www.securityfocus.com/bid/44889>

* SECUNIA: 42410

<http://secunia.com/advisories/42410>

* SECUNIA: 42812

<http://secunia.com/advisories/42812>

* VUPEN: ADV-2010-3081

<http://www.vupen.com/english/advisories/2010/3081>

* VUPEN: ADV-2011-0020

<http://www.vupen.com/english/advisories/2011/0020>

* VUPEN: ADV-2011-0021

<http://www.vupen.com/english/advisories/2011/0021>

* VUPEN: ADV-2011-0077

<http://www.vupen.com/english/advisories/2011/0077>

CVE Reference:

CVE-2009-5016 (cve.mitre.org, nvd.nist.gov)

• 19179 PHP Session Serializer Session Data Injection Vulnerability

The default session serializer in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 does not properly handle the PS_UNDEF_MARKER marker, which allows context-dependent attackers to modify arbitrary session variables via a crafted session variable name.

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

References:

* MISC:

<http://php-security.org/2010/05/31/mops-2010-060-php-session-serializer-session-data-injection-vulnerability/index.html>

* DEBIAN: DSA-2089

<http://www.debian.org/security/2010/dsa-2089>

* REDHAT: RHSA-2010:0919

<http://www.redhat.com/support/errata/RHSA-2010-0919.html>

* SUSE: SUSE-SR:2010:017

<http://lists.opensuse.org/opensuse-security-announce/2010-09/msg00006.html>

* SUSE: SUSE-SR:2010:018

<http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00000.html>

* SECUNIA: 42410

<http://secunia.com/advisories/42410>

* VUPEN: ADV-2010-3081

<http://www.vupen.com/english/advisories/2010/3081>

CVE Reference:

CVE-2010-3065 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-0638 Microsoft CVSS 2.0 Score = 9.3

Microsoft Windows does not properly warn the user before enabling additional Human Interface Device (HID) functionality over USB, which allows user-assisted attackers to execute arbitrary programs via crafted USB data, as demonstrated by keyboard and mouse data sent by malware on a smartphone that the user connected to the computer.

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

References:

MISC: <http://www.cs.gmu.edu/~astavrou/publications.html>

MISC: <http://www.blackhat.com/html/bh-dc-11/bh-dc-11-briefings.html#Stavrou>

MISC: http://news.cnet.com/8301-27080_3-20028919-245.html

CVE Reference: [CVE-2011-0638](http://cve.mitre.org)

• CVE-2011-0273 HP CVSS 2.0 Score = 9.3

Buffer overflow in crs.exe in HP OpenView Storage Data Protector Cell Manager 6.11 allows remote attackers to execute arbitrary code via unspecified message types.

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

References:

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02688353

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02688353

SECTRAK: <http://securitytracker.com/id?1024983>

SECUNIA: <http://secunia.com/advisories/42997>

CVE Reference: [CVE-2011-0273](#)

• **CVE-2011-0274 HP CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in HP Business Availability Center (BAC) 7.x through 7.55 and 8.x through 8.05, and Business Service Management (BSM) through 9.01, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2011/0188>

BID: <http://www.securityfocus.com/bid/45944>

SECTRAK: <http://securitytracker.com/id?1024986>

SECUNIA: <http://secunia.com/advisories/43018>

SECUNIA: <http://secunia.com/advisories/43014>

HP: <http://marc.info/?l=bugtraq&m=129562482815203&w=2>

HP: <http://marc.info/?l=bugtraq&m=129562482815203&w=2>

CVE Reference: [CVE-2011-0274](#)

• **CVE-2011-0637 IBM CVSS 2.0 Score = 4.9**

The FC SCSI protocol driver in IBM AIX 6.1 does not verify that a timer is unused before deallocating this timer, which might allow attackers to cause a denial of service (system crash) via unspecified vectors.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2011/0176>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=isg1I292478>

SECUNIA: <http://secunia.com/advisories/42962>

CVE Reference: [CVE-2011-0637](#)

• **CVE-2011-0352 Cisco CVSS 2.0 Score = 7.8**

Buffer overflow in the web-based management interface on the Cisco Linksys WRT54GC router with firmware before 1.06.1 allows remote attackers to cause a denial of service (device crash) via a long string in a POST request.

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

References:

CONFIRM: <http://tools.cisco.com/security/center/viewAlert.x?alertId=22228>

SECUNIA: <http://secunia.com/advisories/43017>

JVNDB: <http://jvndb.jvn.jp/en/contents/2011/JVNDB-2011-000007.html>

JVN: <http://jvn.jp/en/jp/JVN26605630/index.html>

CVE Reference: [CVE-2011-0352](#)

• **CVE-2011-0639 Apple CVSS 2.0 Score = 9.3**

Apple Mac OS X does not properly warn the user before enabling additional Human Interface Device (HID) functionality over USB, which allows user-assisted attackers to execute arbitrary programs via crafted USB data, as demonstrated by keyboard and mouse data sent by malware on a smartphone that the user connected to the computer.

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

References:

MISC: <http://www.cs.gmu.edu/~astavrou/publications.html>

MISC: <http://www.blackhat.com/html/bh-dc-11/bh-dc-11-briefings.html#Stavrou>

MISC: http://news.cnet.com/8301-27080_3-20028919-245.html

CVE Reference: [CVE-2011-0639](#)

• **CVE-2011-0640 Linux CVSS 2.0 Score = 9.3**

The default configuration of udev on Linux does not warn the user before enabling additional Human Interface Device (HID) functionality over USB, which allows user-assisted attackers to execute arbitrary programs via crafted USB data, as demonstrated by keyboard and mouse data sent by malware on a smartphone that the user connected to the computer.

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

References:

MISC: <http://www.cs.gmu.edu/~astavrou/publications.html>

MISC: <http://www.blackhat.com/html/bh-dc-11/bh-dc-11-briefings.html#Stavrou>

MISC: http://news.cnet.com/8301-27080_3-20028919-245.html

CVE Reference: [CVE-2011-0640](#)

• **CVE-2010-4243 Linux CVSS 2.0 Score = 4.9**

fs/exec.c in the Linux kernel before 2.6.37 does not enable the OOM Killer to assess use of stack memory by arrays representing the (1) arguments and (2) environment, which allows local users to cause a denial of service (memory consumption) via a crafted exec system call, aka an "OOM dodging issue," a related issue to CVE-2010-3858.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=625688

MLIST: <http://openwall.com/lists/oss-security/2010/11/22/15>

MLIST: <http://lkml.org/lkml/2010/8/29/206>

MLIST: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2010-11/msg13278.html>

CONFIRM: <http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=3c77f845722158206a7209c45ccddc264d19319c>

XF: <http://xforce.iss.net/xforce/xfdb/64700>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.37>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/15619>

MLIST: <http://openwall.com/lists/oss-security/2010/11/22/6>

MLIST: <http://lkml.org/lkml/2010/8/30/378>

MLIST: <http://lkml.org/lkml/2010/8/30/138>

MLIST: <http://lkml.org/lkml/2010/8/27/429>

MISC: http://grsecurity.net/~spender/64bit_dos.c

CVE Reference: [CVE-2010-4243](#)

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