

## 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

We start the year with prognosis. Another fraud ring under investigation. Warning from Microsoft. It's a war out there.

Enjoy reading & Stay safe.

**Call or email netVigilance to get an update on SecureScout.**

**(503) 524 5758 or [sales@netVigilance.com](mailto:sales@netvigilance.com)**

## Top Security News Stories this Week

### • 2011 Outlook: Better than 2010 and really wild

Network World - Well my friends, 2010 was quite a year and as is our want, in this, the first issue of the New Year, we throw caution to the winds, dust off our crystal balls and, seeing as we're all consenting adults, indulge in a little hardcore prognostication. But before we head off into the wild blue yonder, let's take a look at my forecasting for last year.

I began with generalities (always a safe way to go), opining that 2010 would be "the year of recovery, the year of realigning that which needs aligning, along with cleaning up what's dirty, polishing up what's tarnished, primping up what's, er, unprimed, and primping up that which is unpimped. In short, generally getting ourselves out of the morass of negativity and gloom that was 2009."

In a broad sense I think I was right on this (I get one point) but the recovery has definitely been softer than expected and my thought that "confidence is going to be erratic" was pretty much spot on (I get another point). Computerworld

Full Story :

[http://www.computerworld.com/s/article/9202962/2011\\_Outlook\\_Better\\_than\\_2010\\_and\\_really\\_wild?source=rss\\_sec](http://www.computerworld.com/s/article/9202962/2011_Outlook_Better_than_2010_and_really_wild?source=rss_sec)

## • DHS zeroing in on Vietnamese-based fraud ring

The U.S. Department of Homeland Security (DHS) has zeroed in on two Vietnamese foreign exchange students believed to be part of an international criminal operation that has duped U.S. retailers out of millions of dollars. Early last month federal investigators raided the Minnesota home of Winona State University students Tram Vo and Khoi Van, both 22, and seized computers, thumb drives, documents and other items.

The investigation, called Operation eMule, began in September 2009 and is targeting a Vietnamese-based international fraud gang made up of numerous individuals in different roles - including computer hackers, fraud managers and sellers of stolen personal identity and financial information, according to a search warrant affidavit obtained by the Minnesota Star Tribune, which first reported on the investigation. The fraud operation also relies on an extensive ring of money transfer mules in the United States. SC Magazine

Full Story :

[http://www.scmagazineus.com/dhs-zeroing-in-on-vietnamese-based-fraud-ring/article/193645/?utm\\_source=feedburn](http://www.scmagazineus.com/dhs-zeroing-in-on-vietnamese-based-fraud-ring/article/193645/?utm_source=feedburn)

## • Microsoft advises of zero-day flaw in its Graphics Engine

Microsoft is warning of an unpatched vulnerability in its Windows Graphics Rendering Engine, which supports image formats, that could lead to remote code execution.

The flaw can enable an attacker to install malicious programs, access data or create accounts with full user rights, according to an advisory released Tuesday.

"To target this vulnerability, an attacker must convince a user to visit a specially crafted malicious web page, or to open a malicious Word or PowerPoint file,"&nbsp;Angela Gunn, senior marketing communications manager for Microsoft Trustworthy Computing, wrote on a company blog post. "Furthermore, users whose accounts are configured to have fewer user rights on the system would be less affected by an attack than those running with administrative rights."&nbsp; SC Magazine

Full Story :

[http://www.scmagazineus.com/microsoft-advises-of-zero-day-flaw-in-its-graphics-engine/article/193682/?utm\\_source=feedburn](http://www.scmagazineus.com/microsoft-advises-of-zero-day-flaw-in-its-graphics-engine/article/193682/?utm_source=feedburn)

## • Bank of America braces itself for fallout from WikiLeaks disclosures, report says

Computerworld - Bank of America has assembled a 15- to 20-person team to come up with a damage control plan in the event Wikileaks follows through on its promise to release thousands of insider documents leaked to it, according to reports.

The team headed by Bruce Thompson, Bank of America's chief risk officer, has launched a broad internal investigation to determine what internal documents have been leaked to the whistleblower Web site, the New York Times reported yesterday.

The group has studied thousands of documents, and is now in the process of reviewing every report of a missing or compromised computer, the newspaper said. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9203180/Bank\\_of\\_America\\_braces\\_itself\\_for\\_fallout\\_from\\_WikiLeaks\\_disclosures](http://www.computerworld.com/s/article/9203180/Bank_of_America_braces_itself_for_fallout_from_WikiLeaks_disclosures)

# New Vulnerabilities Tested in SecureScout

## • 19124 FlashPix Image Converter Heap Corruption Vulnerability (MS10-105/968095) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office parses specially crafted FlashPix image files. The vulnerability could allow remote code execution if a user opens an Office document containing a specially crafted FlashPix image. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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:

\* VUPEN: VUPEN/ADV-2010-3227

<http://www.vupen.com/english/advisories/2010/3227>

\* SECTRACK: 1024887

<http://securitytracker.com/id?1024887>

\* BID: 45283

<http://www.securityfocus.com/bid/45283>

\* MS: MS10-105

<http://www.microsoft.com/technet/security/Bulletin/MS10-105.msp>

#### CVE Reference:

CVE-2010-3952 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19125 PHP double free in imap extension Vulnerability

Double free vulnerability in the `imap_do_open` function in the IMAP extension (`ext/imap/php_imap.c`) in PHP 5.2 before 5.2.15 and 5.3 before 5.3.4 allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.

The issue has been fixed in PHP versions 5.2.15 and 5.3.4.

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

#### References:

\* CONFIRM:

<http://svn.php.net/viewvc?view=revision&revision=305032>

\* CONFIRM:

[https://bugzilla.redhat.com/show\\_bug.cgi?id=656917](https://bugzilla.redhat.com/show_bug.cgi?id=656917)

\* MANDRIVA: MDVSA-2010:239

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:239>

\* BID: 44980

<http://www.securityfocus.com/bid/44980>

\* SECTRACK: 1024761

<http://www.securitytracker.com/id?1024761>

\* VUPEN: ADV-2010-3027

<http://www.vupen.com/english/advisories/2010/3027>

\* XF: php-phpimapc-dos(63390)

<http://xforce.iss.net/xfdb/63390>

\* CONFIRM:

<http://www.php.net/ChangeLog-5.php#5.3.4>

#### CVE Reference:

CVE-2010-4150 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19126 PHP NULL pointer dereference in ZipArchive::getArchiveComment Vulnerability

The `ZipArchive::getArchiveComment` function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ZIP archive.

The issue has been fixed in PHP versions 5.2.15 and 5.3.4.

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

#### References:

\* CONFIRM:

<http://www.php.net/ChangeLog-5.php#5.3.4>

\* SREASONRES: 20101105 PHP 5.3.3/5.2.14 ZipArchive::getArchiveComment NULL Pointer Dereference

[http://securityreason.com/achievement\\_securityalert/90](http://securityreason.com/achievement_securityalert/90)

\* EXPLOIT-DB: 15431

<http://www.exploit-db.com/exploits/15431>

\* CONFIRM:

[http://svn.php.net/viewvc/php/php-src/branches/PHP\\_5\\_2/ext/zip/php\\_zip.c?view=log](http://svn.php.net/viewvc/php/php-src/branches/PHP_5_2/ext/zip/php_zip.c?view=log)

\* CONFIRM:

[http://svn.php.net/viewvc/php/php-src/branches/PHP\\_5\\_3/ext/zip/php\\_zip.c?view=log](http://svn.php.net/viewvc/php/php-src/branches/PHP_5_3/ext/zip/php_zip.c?view=log)

\* MANDRIVA: MDVSA-2010:218

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:218>

\* BID: 44718

<http://www.securityfocus.com/bid/44718>

\* SECTRACK: 1024690

<http://www.securitytracker.com/id?1024690>

#### CVE Reference:

CVE-2010-3709 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19127 PHP flaw in open\_basedir

fopen\_wrappers.c in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3 might allow remote attackers to bypass open\_basedir restrictions via vectors related to the length of a filename.

The issue has been fixed in PHP versions 5.2.15 and 5.3.4.

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

#### References:

- \* CONFIRM:  
<http://www.php.net/ChangeLog-5.php#5.3.4>
- \* CONFIRM:  
<http://security-tracker.debian.org/tracker/CVE-2010-3436>
- \* CONFIRM:  
[http://svn.php.net/viewvc/php/php-src/trunk/main/fopen\\_wrappers.c?r1=303824&r2=303823&pathrev=303824](http://svn.php.net/viewvc/php/php-src/trunk/main/fopen_wrappers.c?r1=303824&r2=303823&pathrev=303824)
- \* CONFIRM:  
<http://svn.php.net/viewvc?view=revision&revision=303824>
- \* MANDRIVA: MDVSA-2010:218  
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:218>
- \* BID: 44723  
<http://www.securityfocus.com/bid/44723>

#### CVE Reference:

CVE-2010-3436 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19128 PHP string validation Vulnerability

Format string vulnerability in stream.c in the phar extension in PHP 5.3.x through 5.3.3 allows context-dependent attackers to obtain sensitive information (memory contents) and possibly execute arbitrary code via a crafted phar:// URI that is not properly handled by the phar\_stream\_flush function, leading to errors in the php\_stream\_wrapper\_log\_error function. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-2094.

The issue has been fixed in PHP 5.3.4.

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

#### References:

- \* CONFIRM:  
<http://www.php.net/ChangeLog-5.php#5.3.4>
- \* MISC:  
[http://php-security.org/2010/05/14/mops-2010-024-php-phar\\_stream\\_flush-format-string-vulnerability/index.html](http://php-security.org/2010/05/14/mops-2010-024-php-phar_stream_flush-format-string-vulnerability/index.html)
- \* CONFIRM:  
<http://security-tracker.debian.org/tracker/CVE-2010-2950>
- \* CONFIRM:  
<http://svn.php.net/viewvc?view=revision&revision=302565>
- \* CONFIRM:  
[https://bugzilla.redhat.com/show\\_bug.cgi?id=598537](https://bugzilla.redhat.com/show_bug.cgi?id=598537)
- \* SUSE: SUSE-SR:2010:017  
<http://lists.opensuse.org/opensuse-security-announce/2010-09/msg00006.html>

#### CVE Reference:

CVE-2010-2950 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19129 PHP Segfault in filter\_var with FILTER\_VALIDATE\_EMAIL with large amount of data

Stack consumption vulnerability in the filter\_var function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3, when FILTER\_VALIDATE\_EMAIL mode is used, allows remote attackers to cause a denial of service (memory consumption and application crash) via a long e-mail address string.

The issue has been fixed in PHP versions 5.2.15, and 5.3.4.

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

#### References:

- \* CONFIRM:  
<http://www.php.net/ChangeLog-5.php#5.3.4>
- \* CONFIRM:

<http://bugs.php.net/bug.php?id=52929>

\* MANDRIVA: MDVSA-2010:218

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:218>

#### CVE Reference:

CVE-2010-3710 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19130 PHP crashes on invalid parameters in intl extension

Integer overflow in the NumberFormatter::getSymbol (aka numfmt\_get\_symbol) function in PHP 5.3.3 and earlier allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument.

The issue has been fixed in PHP version 5.3.4.

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

#### References:

\* CONFIRM:

<http://www.php.net/ChangeLog-5.php#5.3.4>

\* BUGTRAQ: 20101210 PHP 5.3.3 NumberFormatter::getSymbol Integer Overflow

<http://www.securityfocus.com/archive/1/archive/1/515142/100/0/threaded>

\* EXPLOIT-DB: 15722

<http://www.exploit-db.com/exploits/15722>

\* CONFIRM:

[http://svn.php.net/viewvc/php/php-src/trunk/ext/intl/formatter/formatter\\_attr.c?r1=305571&pathrev=305570&r2=305570&pathrev=305571](http://svn.php.net/viewvc/php/php-src/trunk/ext/intl/formatter/formatter_attr.c?r1=305571&pathrev=305570&r2=305570&pathrev=305571)

\* CONFIRM:

<http://svn.php.net/viewvc?view=revision&revision=305571>

\* MANDRIVA: MDVSA-2010:255

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:255>

\* CERT-VN: VU#479900

<http://www.kb.cert.org/vuls/id/479900>

\* BID: 45119

<http://www.securityfocus.com/bid/45119>

#### CVE Reference:

CVE-2010-4409 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19131 PHP mb\_strcut() returns garbage with the excessive length parameter

The mb\_strcut function in Libmbfl 1.1.0, as used in PHP 5.3.x through 5.3.3, allows context-dependent attackers to obtain potentially sensitive information via a large value of the third parameter (aka the length parameter).

The issue has been fixed in PHP version 5.3.4.

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

#### References:

\* CONFIRM:

<http://www.php.net/ChangeLog-5.php#5.3.4>

\* MLIST: [oss-security] 20101107 CVE Request: PHP 5.3.3, libmbfl, mb\_strcut

<http://www.openwall.com/lists/oss-security/2010/11/07/2>

\* MLIST: [oss-security] 20101108 Re: CVE Request: PHP 5.3.3, libmbfl, mb\_strcut

<http://www.openwall.com/lists/oss-security/2010/11/08/13>

\* MISC:

<http://pastie.org/1279428>

\* MISC:

<http://pastie.org/1279682>

\* MANDRIVA: MDVSA-2010:225

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:225>

\* BID: 44727

<http://www.securityfocus.com/bid/44727>

\* SECUNIA: 42135

<http://secunia.com/advisories/42135>

#### CVE Reference:

CVE-2010-4156 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19132 PHP NULL pointer dereference when processing invalid XML-RPC requests

The xmlrpc extension in PHP 5.2.x through 5.2.13 and 5.3.x through 5.3.2 does not properly handle a missing methodName element in the first argument to the xmlrpc\_decode\_request function, which allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) and possibly have unspecified other impact via a crafted argument.

The issue has been fixed in PHP versions 5.2.14, and 5.3.4.

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

#### References:

- \* CONFIRM:  
<http://www.php.net/ChangeLog-5.php#5.3.4>
- \* MLIST: [oss-security] 20100312 CVE-2010-0397: NULL pointer dereference in PHP's xmlrpc extension  
<http://www.openwall.com/lists/oss-security/2010/03/12/5>
- \* CONFIRM:  
<http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=573573>
- \* CONFIRM:  
<http://support.apple.com/kb/HT4312>
- \* CONFIRM:  
<http://support.apple.com/kb/HT4435>
- \* APPLE: APPLE-SA-2010-08-24-1  
<http://lists.apple.com/archives/security-announce/2010/Aug/msg00003.html>
- \* APPLE: APPLE-SA-2010-11-10-1  
<http://lists.apple.com/archives/security-announce/2010/Nov/msg00000.html>
- \* MANDRIVA: MDVSA-2010:068  
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:068>
- \* REDHAT: RHSA-2010:0919  
<http://www.redhat.com/support/errata/RHSA-2010-0919.html>
- \* SUSE: SUSE-SR:2010:012  
<http://lists.opensuse.org/opensuse-security-announce/2010-05/msg00002.html>
- \* SUSE: SUSE-SR:2010:013  
<http://lists.opensuse.org/opensuse-security-announce/2010-06/msg00001.html>
- \* SUSE: SUSE-SR:2010:017  
<http://lists.opensuse.org/opensuse-security-announce/2010-09/msg00006.html>
- \* BID: 38708  
<http://www.securityfocus.com/bid/38708>
- \* SECUNIA: 42410  
<http://secunia.com/advisories/42410>
- \* VUPEN: ADV-2010-0724  
<http://www.vupen.com/english/advisories/2010/0724>
- \* VUPEN: ADV-2010-3081  
<http://www.vupen.com/english/advisories/2010/3081>

#### CVE Reference:

CVE-2010-0397 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19133 PHP possible interruption array leak in strrchr()

The strrchr function in PHP 5.2 before 5.2.14 allows context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler.

The issue has been fixed in PHP 5.2.14.

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

#### References:

- \* CONFIRM:  
<http://www.php.net/ChangeLog-5.php#5.3.4>
- \* CONFIRM:  
[http://www.php.net/releases/5\\_2\\_14.php](http://www.php.net/releases/5_2_14.php)
- \* CONFIRM:  
[https://bugzilla.redhat.com/show\\_bug.cgi?id=619324](https://bugzilla.redhat.com/show_bug.cgi?id=619324)
- \* CONFIRM:  
<http://support.apple.com/kb/HT4312>
- \* CONFIRM:  
<http://support.apple.com/kb/HT4435>
- \* APPLE: APPLE-SA-2010-08-24-1  
<http://lists.apple.com/archives/security-announce/2010/Aug/msg00003.html>
- \* APPLE: APPLE-SA-2010-11-10-1

<http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html>

\* SUSE: SUSE-SR:2010:018

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

#### CVE Reference:

CVE-2010-2484 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

### • CVE-2010-3873 Linux CVSS 2.0 Score = 7.8

The X.25 implementation in the Linux kernel before 2.6.36.2 does not properly parse facilities, which allows remote attackers to cause a denial of service (heap memory corruption and panic) or possibly have unspecified other impact via malformed (1) X25\_FAC\_CALLING\_AE or (2) X25\_FAC\_CALLED\_AE data, related to net/x25/x25\_facilities.c and net/x25/x25\_in.c, a different vulnerability than CVE-2010-4164.

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

#### References:

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=649693](https://bugzilla.redhat.com/show_bug.cgi?id=649693)

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=a6331d6f9a4298173b413cf99a40cc86a9d92c37>

MLIST: <http://www.spinics.net/lists/netdev/msg145873.html>

MLIST: <http://www.spinics.net/lists/netdev/msg145786.html>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.36.2>

MLIST: <http://openwall.com/lists/oss-security/2010/11/04/3>

MLIST: <http://openwall.com/lists/oss-security/2010/11/03/2>

CVE Reference: [CVE-2010-3873](http://cve.mitre.org/cgi-bin/cvehandler.cgi?id=2010-3873)

### • CVE-2010-4164 Linux CVSS 2.0 Score = 7.8

Multiple integer underflows in the x25\_parse\_facilities function in net/x25/x25\_facilities.c in the Linux kernel before 2.6.36.2 allow remote attackers to cause a denial of service (system crash) via malformed X.25 (1) X25\_FAC\_CLASS\_A, (2) X25\_FAC\_CLASS\_B, (3) X25\_FAC\_CLASS\_C, or (4) X25\_FAC\_CLASS\_D facility data, a different vulnerability than CVE-2010-3873.

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

#### References:

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=652517](https://bugzilla.redhat.com/show_bug.cgi?id=652517)

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=5ef41308f94dccb3b7afc56cdef1c2ba53fa5d2f>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.36.2>

MLIST: <http://openwall.com/lists/oss-security/2010/11/12/3>

MLIST: <http://openwall.com/lists/oss-security/2010/11/11/2>

MLIST: <http://marc.info/?l=linux-netdev&m=128951543005554&w=2>

CVE Reference: [CVE-2010-4164](http://cve.mitre.org/cgi-bin/cvehandler.cgi?id=2010-4164)

### • CVE-2010-4162 Linux CVSS 2.0 Score = 4.7

Multiple integer overflows in fs/bio.c in the Linux kernel before 2.6.36.2 allow local users to cause a denial of service (system crash) via a crafted device ioctl to a SCSI device.

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

#### References:

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=652529](https://bugzilla.redhat.com/show_bug.cgi?id=652529)

MLIST: <http://openwall.com/lists/oss-security/2010/11/12/2>

MLIST: <http://openwall.com/lists/oss-security/2010/11/10/18>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=cb4644cac4a2797afc847e6c92736664d4b0ea34>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.36.2>

**CVE Reference:** [CVE-2010-4162](#)

• **CVE-2010-4163 Linux CVSS 2.0 Score = 4.7**

The blk\_rq\_map\_user\_iov function in block/blk-map.c in the Linux kernel before 2.6.36.2 allows local users to cause a denial of service (panic) via a zero-length I/O request in a device ioctl to a SCSI device.

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

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=652957](https://bugzilla.redhat.com/show_bug.cgi?id=652957)

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=9284bcf4e335e5f18a8bc7b26461c33ab60d0689>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.36.2>

MLIST: <http://openwall.com/lists/oss-security/2010/11/29/1>

MLIST: <http://openwall.com/lists/oss-security/2010/11/12/2>

MLIST: <http://openwall.com/lists/oss-security/2010/11/10/18>

**CVE Reference:** [CVE-2010-4163](#)

• **CVE-2010-4668 Linux CVSS 2.0 Score = 4.7**

The blk\_rq\_map\_user\_iov function in block/blk-map.c in the Linux kernel before 2.6.37-rc7 allows local users to cause a denial of service (panic) via a zero-length I/O request in a device ioctl to a SCSI device, related to an unaligned map. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-4163.

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

**References:**

CONFIRM: <https://patchwork.kernel.org/patch/363282/>

MLIST: <http://openwall.com/lists/oss-security/2010/11/30/7>

MLIST: <http://openwall.com/lists/oss-security/2010/11/30/4>

MLIST: <http://openwall.com/lists/oss-security/2010/11/29/1>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=5478755616ae2ef1ce144dded589b62b2a50d575>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.37-rc7>

MLIST: <http://lkml.org/lkml/2010/11/29/70>

MLIST: <http://lkml.org/lkml/2010/11/29/68>

**CVE Reference:** [CVE-2010-4668](#)

• **CVE-2010-3448 Linux CVSS 2.0 Score = 4.0**

drivers/platform/x86/thinkpad\_acpi.c in the Linux kernel before 2.6.34 on ThinkPad devices, when the X.Org X server is used, does not properly restrict access to the video output control state, which allows local users to cause a denial of service (system hang) via a (1) read or (2) write operation.

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

## References:

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=652122](https://bugzilla.redhat.com/show_bug.cgi?id=652122)

MLIST: <http://openwall.com/lists/oss-security/2010/09/30/6>

MLIST: <http://openwall.com/lists/oss-security/2010/09/30/1>

MLIST: <http://openwall.com/lists/oss-security/2010/09/29/7>

MLIST: <http://openwall.com/lists/oss-security/2010/09/28/1>

MLIST: <http://openwall.com/lists/oss-security/2010/06/23/2>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=b525c06cdbc8a3963f0173ccd23f9147d4c384b5>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.34>

CONFIRM: <http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=565790>

**CVE Reference:** [CVE-2010-3448](#)

### • **CVE-2010-3875 Linux CVSS 2.0 Score = 1.9**

The ax25\_getname function in net/ax25/af\_ax25.c in the Linux kernel before 2.6.37-rc2 does not initialize a certain structure, which allows local users to obtain potentially sensitive information from kernel stack memory by reading a copy of this structure.

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

## References:

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=649713](https://bugzilla.redhat.com/show_bug.cgi?id=649713)

MLIST: <http://openwall.com/lists/oss-security/2010/11/04/5>

MLIST: <http://openwall.com/lists/oss-security/2010/11/02/7>

MLIST: <http://marc.info/?l=linux-netdev&m=128854507120898&w=2>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=fe10ae53384e48c51996941b7720ee16995cbcb7>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.37-rc2>

**CVE Reference:** [CVE-2010-3875](#)

### • **CVE-2010-3876 Linux CVSS 2.0 Score = 1.9**

net/packet/af\_packet.c in the Linux kernel before 2.6.37-rc2 does not properly initialize certain structure members, which allows local users to obtain potentially sensitive information from kernel stack memory by leveraging the CAP\_NET\_RAW capability to read copies of the applicable structures.

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

## References:

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=649715](https://bugzilla.redhat.com/show_bug.cgi?id=649715)

MLIST: <http://openwall.com/lists/oss-security/2010/11/04/5>

MLIST: <http://openwall.com/lists/oss-security/2010/11/02/9>

MLIST: <http://openwall.com/lists/oss-security/2010/11/02/7>

MLIST: <http://openwall.com/lists/oss-security/2010/11/02/10>

MLIST: <http://marc.info/?l=linux-netdev&m=128854507220908&w=2>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=67286640f638f5ad41a946b9a3dc75327950248f>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.37-rc2>

MLIST: <http://openwall.com/lists/oss-security/2010/11/02/12>

**CVE Reference:** [CVE-2010-3876](#)

### **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](mailto: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](mailto: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](mailto:info-scanner@securescout.net)