

## 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>

e-symposium on new vulnerabilities. Next generation firewall to be more flexible. Spam levels down after authorities take down botnet. Ransomware on the rise again.

SC Magazine picks netVigilance as Innovator of the Year 2010 in the category vulnerability Assessment.

Peter Stephenson about netVigilance:

**Innovation:** Creative approach to applying vulnerability assessment – both to compliance requirements and true vulnerability management.

**Greatest strength:** Involvement with customer needs and such organizations as NIST, bringing real value to their marketplace.

Read the full story here <http://www.scmagazineus.com/innovators-2010-the-top-security-companies/article/191432/5/>

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

## • Today: SC Magazine eSymposium on New Vulnerabilities

Most successful information thefts are happening because of vulnerabilities in corporate IT infrastructures. Though plugging these holes can be one of the most complex activities for any security team, a plan that addresses this necessary remediation process is critical.

In today's SC Magazine New Vulnerabilities eSymposium, you'll find both educational sessions and opportunities to meet with leading providers in our virtual expo hall to help you address some of the newest vulnerabilities hitting your applications, systems and software.

Various experts will be speaking about the persistent and often complicated challenge of dealing with the unending line of vulnerabilities, zeroing in on some of the more worrisome vulnerabilities that are coming to light and providing some insight on the best action plan to implement for efficient and effective remediation of these holes. SC Magazine

Full Story :

[http://www.scmagazineus.com/today-sc-magazine-esymposium-on-new-vulnerabilities/article/191681/?utm\\_source=](http://www.scmagazineus.com/today-sc-magazine-esymposium-on-new-vulnerabilities/article/191681/?utm_source=)

## • Is a next-generation firewall in your future?

Network World - The traditional port-based enterprise firewall, now looking less like a guard and more like a pit stop for Internet applications racing in through the often open ports 80 and 443, is slowly losing out to a new generation of brawny, fast, intelligent firewalls.

Best practices for cleaning up your firewalls rules base | FAQ: What you should know about Next Generation Firewalls

The so called next-generation firewall (NGFW) describes an enterprise firewall/VPN that has the muscle to efficiently perform intrusion prevention sweeps of traffic, as well as have awareness about the applications moving through it in order to enforce policies based on allowed identity-based application usage. It's supposed to have the brains to use information such as Internet reputation analysis to help with malware filtering or integrate with Active Directory.

Computerworld

Full Story :

[http://www.computerworld.com/s/article/9199021/Is\\_a\\_next\\_generation\\_firewall\\_in\\_your\\_future?source=rss\\_security](http://www.computerworld.com/s/article/9199021/Is_a_next_generation_firewall_in_your_future?source=rss_security)

## • Report: Spam down, but malware continues hold

Spam may be down but malware marches merrily on.

That's the message from the "November Threat Landscape Report" released yesterday by security vendor Fortinet.

Global spam levels ultimately fell 12 percent in November after Dutch authorities took down a large Bredolab network made up of 140 different servers. The Bredolab botnet was typically used by cybercriminals to send out spam selling fake drugs, according to Fortinet. Spam had actually fallen as much as 26 percent the week after the network was dismantled but was able to stage a bit of a recovery afterward. Cnet Security

Full Story :

[http://news.cnet.com/8301-1009\\_3-20024432-83.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-1009_3-20024432-83.html?part=rss&subj=news&tag=2547-1_3-0-20)

## • Ransomware rears ugly head, demands \$120 to unlock files

Computerworld - Ransomware is making a comeback, plaguing users with extortion demands of up to \$120 to return documents or drives to their control, security experts said today.

There appear to be two different campaigns underway, said Chet Wisniewski, a senior security adviser at antivirus vendor Sophos.

"It looks like we're looking at different samples," said Wisniewski, referring to analyses done by Sophos and other security firms, including Kaspersky Lab and CA. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9198743/Ransomware\\_rears\\_ugly\\_head\\_demands\\_120\\_to\\_unlock\\_files?source=rss\\_security](http://www.computerworld.com/s/article/9198743/Ransomware_rears_ugly_head_demands_120_to_unlock_files?source=rss_security)

## New Vulnerabilities Tested in SecureScout

### • 19013 QuickTime stack buffer overflow in error logging (Remote File Checking)

A stack buffer overflow exists in QuickTime's error logging. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This issue is addressed by disabling debug logging. This issue does not affect Mac OS X systems.

The issue has been fixed in version 7.6.7.

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

#### References:

\* CONFIRM:

<http://support.apple.com/kb/HT4290>

\* APPLE: APPLE-SA-2010-08-12-1

<http://lists.apple.com/archives/security-announce/2010//Aug/msg00002.html>

\* BID: 41962

<http://www.securityfocus.com/bid/41962>

\* OVAL: oval:org.mitre.oval:def:11800

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11800>

#### CVE Reference:

CVE-2010-1799 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19075 QuickTime input validation issue (Remote File Checking)

An input validation issue exists in the QuickTime ActiveX control. An optional parameter '\_Marshaled\_pUnk' may be passed to the ActiveX control to specify an arbitrary integer that is later treated as a pointer. Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution. This issue is addressed by ignoring the '\_Marshaled\_pUnk' parameter. This issue does not affect Mac OS X systems.

The issue has been fixed in version 7.6.8.

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

#### References:

\* MISC:

[http://reversemode.com/index.php?option=com\\_content&task=view&id=69&Itemid=1](http://reversemode.com/index.php?option=com_content&task=view&id=69&Itemid=1)

\* MISC:

[http://threatpost.com/en\\_us/blogs/new-remote-flaw-apple-quicktime-bypasses-aslr-and-dep-083010](http://threatpost.com/en_us/blogs/new-remote-flaw-apple-quicktime-bypasses-aslr-and-dep-083010)

\* MISC:

[https://www.metasploit.com/redmine/projects/framework/repository/entry/modules/exploits/windows/browser/apple\\_quicktime](https://www.metasploit.com/redmine/projects/framework/repository/entry/modules/exploits/windows/browser/apple_quicktime)

#### CVE Reference:

CVE-2010-1818 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19076 QuickTime path searching issue exists in Picture Viewer (Remote File Checking)

A path searching issue exists in QuickTime Picture Viewer. If an attacker places a maliciously crafted DLL in the same directory as an image file, opening the image file with QuickTime Picture Viewer may lead to arbitrary code execution. This issue is addressed by removing the current working directory from the DLL search path. This issue does not affect Mac OS X systems.

The issue has been fixed in version 7.6.8.

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

#### References:

\* CONFIRM:

<http://support.apple.com/kb/HT4339>

#### CVE Reference:

CVE-2010-1819 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19077 Mozilla Firefox - Heap buffer overflow mixing document.write and DOM insertion (Remote File Checking)

Morten Krakvik of Telenor SOC reported an exploit targeting particular versions of Firefox 3.6 on Windows XP that Telenor found while investigating an intrusion attempt on a customer network. The underlying vulnerability, however, was present on both the Firefox 3.5 and Firefox 3.6 development branches and affected all supported platforms.

The issue has been fixed in Firefox 3.6.12 and 3.5.15.

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

#### References:

\* MISC:

<http://isc.sans.edu/diary.html?storyid=9817>

\* MISC:

[http://www.norman.com/about\\_norman/press\\_center/news\\_archive/2010/129223/](http://www.norman.com/about_norman/press_center/news_archive/2010/129223/)

\* MISC:

[http://www.norman.com/security\\_center/virus\\_description\\_archive/129146/](http://www.norman.com/security_center/virus_description_archive/129146/)

\* MISC:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=607222#c53](https://bugzilla.mozilla.org/show_bug.cgi?id=607222#c53)

\* MISC:

[http://norman.com/about\\_norman/press\\_center/news\\_archive/2010/129223/en?utm\\_source=twitterfeed&utm\\_medium=](http://norman.com/about_norman/press_center/news_archive/2010/129223/en?utm_source=twitterfeed&utm_medium=)

\* CONFIRM:

<http://blog.mozilla.com/security/2010/10/26/critical-vulnerability-in-firefox-3-5-and-firefox-3-6/>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=607222](https://bugzilla.mozilla.org/show_bug.cgi?id=607222)

\* CONFIRM:

[https://bugzilla.redhat.com/show\\_bug.cgi?id=646997](https://bugzilla.redhat.com/show_bug.cgi?id=646997)

\* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-73.html>

\* CONFIRM:

<http://support.avaya.com/css/P8/documents/100114329>

\* CONFIRM:

<http://support.avaya.com/css/P8/documents/100114335>

\* FEDORA: FEDORA-2010-17105

<http://lists.fedoraproject.org/pipermail/package-announce/2010-November/050233.html>

\* FEDORA: FEDORA-2010-16883

<http://lists.fedoraproject.org/pipermail/package-announce/2010-October/050061.html>

\* MANDRIVA: MDVSA-2010:213

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:213>

\* MANDRIVA: MDVSA-2010:219

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:219>

\* REDHAT: RHSA-2010:0809

<http://www.redhat.com/support/errata/RHSA-2010-0809.html>

\* REDHAT: RHSA-2010:0810

<http://www.redhat.com/support/errata/RHSA-2010-0810.html>

\* REDHAT: RHSA-2010:0808

<http://www.redhat.com/support/errata/RHSA-2010-0808.html>

\* REDHAT: RHSA-2010:0812

<https://rhn.redhat.com/errata/RHSA-2010-0812.html>

\* SLACKWARE: SSA:2010-305-01

<http://slackware.com/security/viewer.php?l=slackware-security&y=2010&m=slackware-security.556706>

\* UBUNTU: USN-1011-3

<http://www.ubuntu.com/usn/USN-1011-3>

\* UBUNTU: USN-1011-1

<http://www.ubuntu.com/usn/usn-1011-1>

\* BID: 44425

<http://www.securityfocus.com/bid/44425>

\* SECTRACK: 1024650

<http://www.securitytracker.com/id?1024650>

\* SECTRACK: 1024651

<http://www.securitytracker.com/id?1024651>

\* SECTRACK: 1024645

<http://www.securitytracker.com/id?1024645>

\* SECUNIA: 41966

<http://secunia.com/advisories/41966>

\* SECUNIA: 41969

<http://secunia.com/advisories/41969>

\* SECUNIA: 42008

<http://secunia.com/advisories/42008>

\* SECUNIA: 42043

<http://secunia.com/advisories/42043>

\* SECUNIA: 41761

<http://secunia.com/advisories/41761>

\* SECUNIA: 41965

<http://secunia.com/advisories/41965>

\* SECUNIA: 41975

<http://secunia.com/advisories/41975>

\* SECUNIA: 42003

<http://secunia.com/advisories/42003>

\* VUPEN: ADV-2010-2871

<http://www.vupen.com/english/advisories/2010/2871>

\* VUPEN: ADV-2010-2837

<http://www.vupen.com/english/advisories/2010/2837>

\* VUPEN: ADV-2010-2857

<http://www.vupen.com/english/advisories/2010/2857>

\* VUPEN: ADV-2010-2864

<http://www.vupen.com/english/advisories/2010/2864>

#### CVE Reference:

CVE-2010-3765 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19078 Mozilla Thunderbird - Heap buffer overflow mixing document.write and DOM insertion (Remote File Checking)

Morten Krakvik of Telenor SOC reported an exploit targeting particular versions of Thunderbird on Windows XP that Telenor found while investigating an intrusion attempt on a customer network. The underlying vulnerability, however, was present on both the Firefox 3.5 and Firefox 3.6 development branches and affected all supported platforms.

The issue has been fixed in Thunderbird 3.1.6 and 3.0.10.

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

#### References:

\* MISC:

<http://isc.sans.edu/diary.html?storyid=9817>

\* MISC:

[http://www.norman.com/about\\_norman/press\\_center/news\\_archive/2010/129223/](http://www.norman.com/about_norman/press_center/news_archive/2010/129223/)

\* MISC:

[http://www.norman.com/security\\_center/virus\\_description\\_archive/129146/](http://www.norman.com/security_center/virus_description_archive/129146/)

\* MISC:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=607222#c53](https://bugzilla.mozilla.org/show_bug.cgi?id=607222#c53)

\* MISC:

[http://norman.com/about\\_norman/press\\_center/news\\_archive/2010/129223/en?utm\\_source=twitterfeed&utm\\_medium=](http://norman.com/about_norman/press_center/news_archive/2010/129223/en?utm_source=twitterfeed&utm_medium=)

\* CONFIRM:

<http://blog.mozilla.com/security/2010/10/26/critical-vulnerability-in-firefox-3-5-and-firefox-3-6/>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=607222](https://bugzilla.mozilla.org/show_bug.cgi?id=607222)

\* CONFIRM:

[https://bugzilla.redhat.com/show\\_bug.cgi?id=646997](https://bugzilla.redhat.com/show_bug.cgi?id=646997)

\* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-73.html>

\* CONFIRM:

<http://support.avaya.com/css/P8/documents/100114329>

\* CONFIRM:

<http://support.avaya.com/css/P8/documents/100114335>

\* FEDORA: FEDORA-2010-17105

<http://lists.fedoraproject.org/pipermail/package-announce/2010-November/050233.html>

\* FEDORA: FEDORA-2010-16883

<http://lists.fedoraproject.org/pipermail/package-announce/2010-October/050061.html>

\* MANDRIVA: MDVSA-2010:213

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:213>

\* MANDRIVA: MDVSA-2010:219

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:219>

\* REDHAT: RHSA-2010:0809

<http://www.redhat.com/support/errata/RHSA-2010-0809.html>

\* REDHAT: RHSA-2010:0810

<http://www.redhat.com/support/errata/RHSA-2010-0810.html>

\* REDHAT: RHSA-2010:0808

<http://www.redhat.com/support/errata/RHSA-2010-0808.html>

\* REDHAT: RHSA-2010:0812

<https://rhn.redhat.com/errata/RHSA-2010-0812.html>

\* SLACKWARE: SSA:2010-305-01

<http://slackware.com/security/viewer.php?l=slackware-security&y=2010&m=slackware-security.556706>

\* UBUNTU: USN-1011-3

<http://www.ubuntu.com/usn/USN-1011-3>

\* UBUNTU: USN-1011-1

<http://www.ubuntu.com/usn/usn-1011-1>

\* BID: 44425

<http://www.securityfocus.com/bid/44425>

\* SECTRACK: 1024650  
<http://www.securitytracker.com/id?1024650>  
\* SECTRACK: 1024651  
<http://www.securitytracker.com/id?1024651>  
\* SECTRACK: 1024645  
<http://www.securitytracker.com/id?1024645>  
\* SECUNIA: 41966  
<http://secunia.com/advisories/41966>  
\* SECUNIA: 41969  
<http://secunia.com/advisories/41969>  
\* SECUNIA: 42008  
<http://secunia.com/advisories/42008>  
\* SECUNIA: 42043  
<http://secunia.com/advisories/42043>  
\* SECUNIA: 41761  
<http://secunia.com/advisories/41761>  
\* SECUNIA: 41965  
<http://secunia.com/advisories/41965>  
\* SECUNIA: 41975  
<http://secunia.com/advisories/41975>  
\* SECUNIA: 42003  
<http://secunia.com/advisories/42003>  
\* VUPEN: ADV-2010-2871  
<http://www.vupen.com/english/advisories/2010/2871>  
\* VUPEN: ADV-2010-2837  
<http://www.vupen.com/english/advisories/2010/2837>  
\* VUPEN: ADV-2010-2857  
<http://www.vupen.com/english/advisories/2010/2857>  
\* VUPEN: ADV-2010-2864  
<http://www.vupen.com/english/advisories/2010/2864>

#### CVE Reference:

CVE-2010-3765 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19079 Mozilla Firefox - Unsafe library loading vulnerabilities (Remote File Checking)

Mozilla developer Ehsan Akhgari reported that a function used to load external libraries on Windows platforms was using a relative path to a DLL-loading application and was thus vulnerable to binary planting if an attacker was able to place an executable of the same name in the current working directory or any of the other locations that Windows searches for executables.

The issue has been fixed in Firefox 3.6.11 and 3.5.14.

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

#### References:

\* CONFIRM:  
<http://www.mozilla.org/security/announce/2010/mfsa2010-71.html>  
\* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=589190](https://bugzilla.mozilla.org/show_bug.cgi?id=589190)

#### CVE Reference:

CVE-2010-3181 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19080 Mozilla Thunderbird - Unsafe library loading vulnerabilities (Remote File Checking)

Mozilla developer Ehsan Akhgari reported that a function used to load external libraries on Windows platforms was using a relative path to a DLL-loading application and was thus vulnerable to binary planting if an attacker was able to place an executable of the same name in the current working directory or any of the other locations that Windows searches for executables.

The issue has been fixed in Thunderbird 3.1.5 and 3.0.9.

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

#### References:

\* CONFIRM:  
<http://www.mozilla.org/security/announce/2010/mfsa2010-71.html>  
\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=589190](https://bugzilla.mozilla.org/show_bug.cgi?id=589190)

**CVE Reference:**

CVE-2010-3181 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **19081 Mozilla Thunderbird - SSL wildcard certificate matching IP addresses (Remote File Checking)**

Security researcher Richard Moore reported that when an SSL certificate was created with a common name containing a wildcard followed by a partial IP address a valid SSL connection could be established with a server whose IP address matched the wildcard range by browsing directly to the IP address. It is extremely unlikely that such a certificate would be issued by a Certificate Authority.

The issue has been fixed in Thunderbird 3.1.5 and 3.0.9.

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

**References:**

\* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-70.html>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=578697](https://bugzilla.mozilla.org/show_bug.cgi?id=578697)

\* MANDRIVA: MDVSA-2010:210

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:210>

\* REDHAT: RHSA-2010:0781

<http://www.redhat.com/support/errata/RHSA-2010-0781.html>

\* REDHAT: RHSA-2010:0782

<http://www.redhat.com/support/errata/RHSA-2010-0782.html>

\* UBUNTU: USN-1007-1

<http://www.ubuntu.com/usn/USN-1007-1>

\* SECUNIA: 41839

<http://secunia.com/advisories/41839>

**CVE Reference:**

CVE-2010-3170 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **19082 Mozilla Firefox - SSL wildcard certificate matching IP addresses (Remote File Checking)**

Security researcher Richard Moore reported that when an SSL certificate was created with a common name containing a wildcard followed by a partial IP address a valid SSL connection could be established with a server whose IP address matched the wildcard range by browsing directly to the IP address. It is extremely unlikely that such a certificate would be issued by a Certificate Authority.

The issue has been fixed in Firefox 3.6.11 and 3.5.14.

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

**References:**

\* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-70.html>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=578697](https://bugzilla.mozilla.org/show_bug.cgi?id=578697)

\* MANDRIVA: MDVSA-2010:210

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:210>

\* REDHAT: RHSA-2010:0781

<http://www.redhat.com/support/errata/RHSA-2010-0781.html>

\* REDHAT: RHSA-2010:0782

<http://www.redhat.com/support/errata/RHSA-2010-0782.html>

\* UBUNTU: USN-1007-1

<http://www.ubuntu.com/usn/USN-1007-1>

\* SECUNIA: 41839

<http://secunia.com/advisories/41839>

**CVE Reference:**

CVE-2010-3170 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **19083 Mozilla Firefox - Cross-site information disclosure via modal calls (Remote File Checking)**

Security researcher Eduardo Vela Nava reported that if a web page opened a new window and used a javascript: URL to make a modal call, such as alert(), then subsequently navigated the page to a different domain, once the modal call

returned the opener of the window could get access to objects in the navigated window. This is a violation of the same-origin policy and could be used by an attacker to steal information from another web site.

The issue has been fixed in Firefox 3.6.11 and 3.5.14.

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

#### References:

\* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-69.html>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=576616](https://bugzilla.mozilla.org/show_bug.cgi?id=576616)

\* MANDRIVA: MDVSA-2010:210

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:210>

\* MANDRIVA: MDVSA-2010:211

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:211>

\* REDHAT: RHSA-2010:0782

<http://www.redhat.com/support/errata/RHSA-2010-0782.html>

#### CVE Reference:

CVE-2010-3178 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

### • CVE-2010-4354 Cisco CVSS 2.0 Score = 5.0

The remote-access IPSec VPN implementation on Cisco Adaptive Security Appliances (ASA) 5500 series devices, PIX Security Appliances 500 series devices, and VPN Concentrators 3000 series devices responds to an Aggressive Mode IKE Phase I message only when the group name is configured on the device, which allows remote attackers to enumerate valid group names via a series of IKE negotiation attempts, aka Bug ID CSCtj96108, a different vulnerability than CVE-2005-2025.

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

#### References:

CISCO: [http://www.cisco.com/en/US/products/products\\_security\\_response09186a0080b5992c.html](http://www.cisco.com/en/US/products/products_security_response09186a0080b5992c.html)

#### CVE Reference: [CVE-2010-4354](http://cve.mitre.org)

### • CVE-2010-4249 Linux CVSS 2.0 Score = 4.9

The `wait_for_unix_gc` function in `net/unix/garbage.c` in the Linux kernel before 2.6.37-rc3-next-20101125 does not properly select times for garbage collection of inflight sockets, which allows local users to cause a denial of service (system hang) via crafted use of the `socketpair` and `sendmsg` system calls for `SOCK_SEQPACKET` sockets.

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

#### References:

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=656756](https://bugzilla.redhat.com/show_bug.cgi?id=656756)

MLIST: <http://www.openwall.com/lists/oss-security/2010/11/24/10>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/next/patch-v2.6.37-rc3-next-20101125.bz2>

MLIST: <http://marc.info/?l=linux-netdev&m=129059035929046&w=2>

MLIST: <http://lkml.org/lkml/2010/11/23/450>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/davem/net-2.6.git;a=commit;h=9915672d41273f5b77f1b3c29b391ffb7732b84b>

BID: <http://www.securityfocus.com/bid/45037>

MLIST: <http://www.openwall.com/lists/oss-security/2010/11/24/2>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/15622/>

MLIST: <http://lkml.org/lkml/2010/11/25/8>

MLIST: <http://lkml.org/lkml/2010/11/23/395>

**CVE Reference:** [CVE-2010-4249](#)

• **CVE-2010-3858 Linux CVSS 2.0 Score = 4.9**

The setup\_arg\_pages function in fs/exec.c in the Linux kernel before 2.6.36, when CONFIG\_STACK\_GROWSDOWN is used, does not properly restrict the stack memory consumption of the (1) arguments and (2) environment for a 32-bit application on a 64-bit platform, which allows local users to cause a denial of service (system crash) via a crafted exec system call, a related issue to CVE-2010-2240.

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

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=645222](https://bugzilla.redhat.com/show_bug.cgi?id=645222)

MLIST: <http://www.openwall.com/lists/oss-security/2010/10/22/4>

MLIST: <http://www.openwall.com/lists/oss-security/2010/10/21/1>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=1b528181b2ffa14721fb28ad1bd539fe1732c583>

BID: <http://www.securityfocus.com/bid/44301>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.36>

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

MISC: [http://grsecurity.net/~spender/64bit\\_dos.c](http://grsecurity.net/~spender/64bit_dos.c)

**CVE Reference:** [CVE-2010-3858](#)

• **CVE-2010-4248 Linux CVSS 2.0 Score = 4.7**

Race condition in the \_\_exit\_signal function in kernel/exit.c in the Linux kernel before 2.6.37-rc2 allows local users to cause a denial of service via vectors related to multithreaded exec, the use of a thread group leader in kernel/posix-cpu-timers.c, and the selection of a new thread group leader in the de\_thread function in fs/exec.c.

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

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=656264](https://bugzilla.redhat.com/show_bug.cgi?id=656264)

MLIST: <http://www.openwall.com/lists/oss-security/2010/11/24/9>

MLIST: <http://www.openwall.com/lists/oss-security/2010/11/23/2>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=e0a70217107e6f9844628120412cb27bb4cea194>

BID: <http://www.securityfocus.com/bid/45028>

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

**CVE Reference:** [CVE-2010-4248](#)

• **CVE-2010-4072 Linux CVSS 2.0 Score = 1.9**

The copy\_shmid\_to\_user function in ipc/shm.c in the Linux kernel before 2.6.37-rc1 does not initialize a certain structure, which allows local users to obtain potentially sensitive information from kernel stack memory via vectors related to the shmctl system call and the "old shm interface."

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

**References:**

MLIST: <http://lkml.org/lkml/2010/10/6/454>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=3af54c9bd9e6f14f896aac1bb0e8405ae0bc7a44>

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=648656](https://bugzilla.redhat.com/show_bug.cgi?id=648656)

MLIST: <http://www.openwall.com/lists/oss-security/2010/10/25/3>

MLIST: <http://www.openwall.com/lists/oss-security/2010/10/07/1>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.37-rc1>

**CVE Reference:** [CVE-2010-4072](#)

• **CVE-2010-4073 Linux CVSS 2.0 Score = 1.9**

The ipc subsystem in the Linux kernel before 2.6.37-rc1 does not initialize certain structures, which allows local users to obtain potentially sensitive information from kernel stack memory via vectors related to the (1) compat\_sys\_semctl, (2) compat\_sys\_msgctl, and (3) compat\_sys\_shmctl functions in ipc/compat.c; and the (4) compat\_sys\_mq\_open and (5) compat\_sys\_mq\_getsetattr functions in ipc/compat\_mq.c.

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

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=648658](https://bugzilla.redhat.com/show_bug.cgi?id=648658)

MLIST: <http://www.openwall.com/lists/oss-security/2010/10/25/3>

MLIST: <http://www.openwall.com/lists/oss-security/2010/10/07/1>

MLIST: <http://lkml.org/lkml/2010/10/6/492>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=03145beb455cf5c20a761e8451e30b8a74ba58d9>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.37-rc1>

**CVE Reference:** [CVE-2010-4073](#)

• **CVE-2010-4074 Linux CVSS 2.0 Score = 1.9**

The USB subsystem in the Linux kernel before 2.6.36-rc5 does not properly initialize certain structure members, which allows local users to obtain potentially sensitive information from kernel stack memory via vectors related to TIOCGICOUNT ioctl calls, and the (1) mos7720\_ioctl function in drivers/usb/serial/mos7720.c and (2) mos7840\_ioctl function in drivers/usb/serial/mos7840.c.

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

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=648659](https://bugzilla.redhat.com/show_bug.cgi?id=648659)

MLIST: <http://www.openwall.com/lists/oss-security/2010/10/25/3>

MLIST: <http://www.openwall.com/lists/oss-security/2010/10/07/1>

MLIST: <http://www.openwall.com/lists/oss-security/2010/09/25/2>

MLIST: <http://lkml.org/lkml/2010/9/15/392>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=a0846f1868b11cd827bdfeaf4527d8b1b1c0b098>

MLIST: <http://www.openwall.com/lists/oss-security/2010/10/06/6>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/testing/v2.6.36/ChangeLog-2.6.36-rc5>

**CVE Reference:** [CVE-2010-4074](#)

• **CVE-2010-4075 Linux CVSS 2.0 Score = 1.9**

The uart\_get\_count function in drivers/serial/serial\_core.c in the Linux kernel before 2.6.37-rc1 does not properly initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel stack memory via a TIOCGICOUNT ioctl call.

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

#### **References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=648660](https://bugzilla.redhat.com/show_bug.cgi?id=648660)

MLIST: <http://www.openwall.com/lists/oss-security/2010/10/25/3>

MLIST: <http://www.openwall.com/lists/oss-security/2010/10/07/1>

MLIST: <http://www.openwall.com/lists/oss-security/2010/09/25/2>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=d281da7ff6f70efca0553c288bb883e8605b3862>

MLIST: <http://www.openwall.com/lists/oss-security/2010/10/06/6>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.37-rc1>

MLIST: <http://lkml.indiana.edu/hypermail/linux/kernel/1009.1/03388.html>

**CVE Reference:** [CVE-2010-4075](https://cve.mitre.org/cgi-bin/cvename.cgi?id=CVE-2010-4075)

#### **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)