

## 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://www2.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

## This Week in Review

Dutch ssl provider seriously breached. The cost of cyber crime. Microsoft to release critical security patches.

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

### • DigiNotar breach fallout widens as more details emerge

The Netherlands-based certificate authority (CA) DigiNotar operated with glaring security weaknesses, including a lack of anti-virus software on certain servers, which permitted hackers to create and issue 531 counterfeit certificates for a myriad of high-profile websites, according to a report released Monday.

The report, from security firm Fox-IT and commissioned by the Dutch government, found that DigiNotar's network infrastructure lacked basic protection mechanisms. Specifically, the investigation found that the most critical servers contained undetectable malware, were accessible via the local area network and were protected by passwords that "could easily be brute-forced." In addition, the servers contained unpatched software and lacked anti-virus defenses.

"The successful hack implies that the current network setup and/or procedures at DigiNotar are not sufficiently secure to prevent this kind of attack," according to the report. "The network has been severely breached." SC Magazine

Full Story :

[http://www.scmagazineus.com/diginotar-breach-fallout-widens-as-more-details-emerge/article/211349/?utm\\_source=](http://www.scmagazineus.com/diginotar-breach-fallout-widens-as-more-details-emerge/article/211349/?utm_source=)

## • Cybercrime costs \$388B annually, report says

Cybercrime has affected 431 million adults around the world in the past year and cost \$388 billion in monetary and time losses, according to the "2011 Norton Cybercrime Report," released Wednesday by Symantec. The report, based on interviews with nearly 20,000 individuals from 24 countries, found that 14 adults become victims of cybercrime every second, totaling more than one million victims each day. In the United States alone, digital offenses cost victims more than \$139 million in cash costs and lost time over the past year.

Overall, 69 percent of adult users have experienced cybercrime in their lifetime, according to the report. Viruses and malware are the most common - and preventable - type of crime, followed by online scams and phishing. SC Magazine

Full Story :

[http://www.scmagazineus.com/cybercrime-costs-388b-annually-report-says/article/211431/?utm\\_source=feedburner](http://www.scmagazineus.com/cybercrime-costs-388b-annually-report-says/article/211431/?utm_source=feedburner)

## • Microsoft, Adobe announce forthcoming patches

Microsoft and Adobe are both planning to release security updates on Tuesday, the companies announced.

As part of its monthly Patch Tuesday updates, Microsoft is readying five security bulletins - all rated "important" - to address 15 vulnerabilities, the company said in its advance notification, released Thursday.

None of the bulletins to be released on Tuesday are rated "critical," Microsoft's highest level of severity reserved for flaws that could allow the propagation of a worm without user action. SC Magazine

Full Story :

[http://www.scmagazineus.com/microsoft-adobe-announce-forthcoming-patches/article/211504/?utm\\_source=feedburner](http://www.scmagazineus.com/microsoft-adobe-announce-forthcoming-patches/article/211504/?utm_source=feedburner)

## New Vulnerabilities Tested in SecureScout

### • 19451 Mozilla Firefox - Unsigned scripts can call script inside signed JAR (Remote File Checking)

The implementation of digital signatures for JAR files in Mozilla Firefox 4.x through 5 and possibly other products does not prevent calls from unsigned JavaScript code to signed code, which allows remote attackers to bypass the Same Origin Policy and gain privileges via a crafted web site, a different vulnerability than CVE-2008-2801.

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

#### References:

\* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=657267](https://bugzilla.mozilla.org/show_bug.cgi?id=657267)

\* BID: 49248

<http://www.securityfocus.com/bid/49248>

#### CVE Reference:

CVE-2011-2993 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19452 Mozilla Firefox - Miscellaneous memory safety hazards (CVE-2011-2989) (Remote File Checking)

The browser engine in Mozilla Firefox 4.x through 5, SeaMonkey 2.x before 2.3 and possibly other products does not properly implement WebGL, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.

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

#### References:

\* BID: 49248

<http://www.securityfocus.com/bid/49248>

\* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=674042](https://bugzilla.mozilla.org/show_bug.cgi?id=674042)

#### CVE Reference:

CVE-2011-2989 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### ● 19453 Mozilla Firefox - Miscellaneous memory safety hazards (CVE-2011-2991) (Remote File Checking)

The browser engine in Mozilla Firefox 4.x through 5, SeaMonkey 2.x before 2.3 and possibly other products does not properly implement WebGL, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.

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

#### References:

- \* BID: 49243  
<http://www.securityfocus.com/bid/49243>
- \* CONFIRM:  
<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>
- \* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=655660](https://bugzilla.mozilla.org/show_bug.cgi?id=655660)

#### CVE Reference:

CVE-2011-2991 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### ● 19454 Mozilla Firefox - Miscellaneous memory safety hazards (CVE-2011-2992) (Remote File Checking)

The Ogg reader in the browser engine in Mozilla Firefox 4.x through 5, Thunderbird before 6, and possibly other products allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.

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

#### References:

- \* BID: 49245  
<http://www.securityfocus.com/bid/49245>
- \* CONFIRM:  
<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>
- \* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=672789](https://bugzilla.mozilla.org/show_bug.cgi?id=672789)

#### CVE Reference:

CVE-2011-2992 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### ● 19455 Mozilla Firefox - Miscellaneous memory safety hazards (CVE-2011-2985) (Remote File Checking)

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 4.x through 5, Thunderbird before 6, before 2.3, and possibly other products allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

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

#### References:

- \* BID: 49224  
<http://www.securityfocus.com/bid/49224>
- \* CONFIRM:  
<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>
- \* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=646825](https://bugzilla.mozilla.org/show_bug.cgi?id=646825)
- \* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=648206](https://bugzilla.mozilla.org/show_bug.cgi?id=648206)
- \* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=650273](https://bugzilla.mozilla.org/show_bug.cgi?id=650273)
- \* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=650275](https://bugzilla.mozilla.org/show_bug.cgi?id=650275)
- \* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=650732](https://bugzilla.mozilla.org/show_bug.cgi?id=650732)
- \* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=651030](https://bugzilla.mozilla.org/show_bug.cgi?id=651030)
- \* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=660517](https://bugzilla.mozilla.org/show_bug.cgi?id=660517)
- \* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=662132](https://bugzilla.mozilla.org/show_bug.cgi?id=662132)

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=665518](https://bugzilla.mozilla.org/show_bug.cgi?id=665518)

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=667092](https://bugzilla.mozilla.org/show_bug.cgi?id=667092)

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=667315](https://bugzilla.mozilla.org/show_bug.cgi?id=667315)

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=667512](https://bugzilla.mozilla.org/show_bug.cgi?id=667512)

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=668245](https://bugzilla.mozilla.org/show_bug.cgi?id=668245)

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=669584](https://bugzilla.mozilla.org/show_bug.cgi?id=669584)

#### CVE Reference:

CVE-2011-2985 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19456 Mozilla Firefox - String crash using WebGL shaders(CVE-2011-2988) (Remote File Checking)

Buffer overflow in an unspecified string class in the WebGL shader implementation in Mozilla Firefox 4.x through 5, Thunderbird before 6, before 2.3, and possibly other products allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a long source-code block for a shader.

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

#### References:

\* BID: 49242

<http://www.securityfocus.com/bid/49242>

\* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=665936](https://bugzilla.mozilla.org/show_bug.cgi?id=665936)

#### CVE Reference:

CVE-2011-2988 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19457 Mozilla Firefox - Crash in SVGTextElement.getCharNumAtPosition()(CVE-2011-0084) (Remote File Checking)

The SVGTextElement.getCharNumAtPosition function in Mozilla Firefox before 3.6.20, and 4.x through 5; Thunderbird 3.x before 3.1.12 and other versions before 6; and possibly other products does not properly handle SVG text, which allows remote attackers to execute arbitrary code via unspecified vectors that lead to a "dangling pointer."

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

#### References:

\* BID: 49213

<http://www.securityfocus.com/bid/49213>

\* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>

\* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-30.html>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=648094](https://bugzilla.mozilla.org/show_bug.cgi?id=648094)

\* DEBIAN: DSA-2295

<http://www.debian.org/security/2011/dsa-2295>

\* DEBIAN: DSA-2296

<http://www.debian.org/security/2011/dsa-2296>

\* REDHAT: RHSA-2011:1164

<http://www.redhat.com/support/errata/RHSA-2011-1164.html>

\* REDHAT: RHSA-2011:1166

<http://www.redhat.com/support/errata/RHSA-2011-1166.html>

#### CVE Reference:

CVE-2011-0084 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19458 Mozilla Firefox - Credential leakage using Content Security Policy reports (CVE-2011-2990) (Remote File Checking)

The implementation of Content Security Policy (CSP) violation reports in Mozilla Firefox 4.x through 5, SeaMonkey 2.x before 2.3, and possibly other products does not remove proxy-authorization credentials from the listed request headers, which allows attackers to obtain sensitive information by reading a report, related to incorrect host resolution that occurs with certain redirects.

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

#### References:

- \* BID: 49246  
<http://www.securityfocus.com/bid/49246>
- \* CONFIRM:  
<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>
- \* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=664983](https://bugzilla.mozilla.org/show_bug.cgi?id=664983)
- \* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=679588](https://bugzilla.mozilla.org/show_bug.cgi?id=679588)

#### CVE Reference:

CVE-2011-2990 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19459 Mozilla Firefox - Cross-origin data theft using canvas and Windows D2D (CVE-2011-2986)(Remote File Checking)

Mozilla Firefox 4.x through 5, Thunderbird before 6, and possibly other products, when the Direct2D (aka D2D) API is used on Windows, allows remote attackers to bypass the Same Origin Policy, and obtain sensitive image data from a different domain, by inserting this data into a canvas.

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

#### References:

- \* BID: 49227  
<http://www.securityfocus.com/bid/49227>
- \* CONFIRM:  
<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>
- \* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=655836](https://bugzilla.mozilla.org/show_bug.cgi?id=655836)

#### CVE Reference:

CVE-2011-2986 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19460 Mozilla Firefox - Heap overflow in ANGLE library (CVE-2011-2987) (Remote File Checking)

Heap-based buffer overflow in Almost Native Graphics Layer Engine (ANGLE), as used in the WebGL implementation in Mozilla Firefox 4.x through 5, Thunderbird before 6, and possibly other products might allow remote attackers to execute arbitrary code via unspecified vectors.

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

#### References:

- \* BID: 49226  
<http://www.securityfocus.com/bid/49226>
- \* CONFIRM:  
<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>
- \* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=665934](https://bugzilla.mozilla.org/show_bug.cgi?id=665934)

#### CVE Reference:

CVE-2011-2987 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

#### • CVE-2011-1359 IBM CVSS 2.0 Score = 5.0

Directory traversal vulnerability in the administration console in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.41, 7.0 before 7.0.0.19, and 8.0 before 8.0.0.1 allows remote attackers to read arbitrary files via a .. (dot dot) in the URI.

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

**References:**

XF: <http://xforce.iss.net/xforce/xfdb/69473>

BID: <http://www.securityfocus.com/bid/49362>

OSVDB: <http://www.osvdb.org/74817>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21509257>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM45322>

SECUNIA: <http://secunia.com/advisories/45749>

**CVE Reference:** [CVE-2011-1359](#)

• **CVE-2011-3390 IBM CVSS 2.0 Score = 4.3**

Multiple cross-site scripting (XSS) vulnerabilities in index.php in IBM OpenAdmin Tool (OAT) before 2.72 for Informix allow remote attackers to inject arbitrary web script or HTML via the (1) informixserver, (2) host, or (3) port parameter in a login action.

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

**References:**

XF: <http://xforce.iss.net/xforce/xfdb/69488>

BID: <http://www.securityfocus.com/bid/49364>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/519468/100/0/threaded>

MISC: <http://voidroot.blogspot.com/2011/08/xss-in-ibm-open-admin-tool.html>

**CVE Reference:** [CVE-2011-3390](#)

• **CVE-2011-0258 Apple CVSS 2.0 Score = 9.3**

Apple QuickTime before 7.7 on Windows allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted image description associated with an mp4v tag in a movie file.

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

**References:**

MISC: <http://zerodayinitiative.com/advisories/ZDI-11-277/>

XF: <http://xforce.iss.net/xforce/xfdb/69518>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/519483/100/0/threaded>

CONFIRM: <http://support.apple.com/kb/HT4826>

**CVE Reference:** [CVE-2011-0258](#)

• **CVE-2011-2654 Novell CVSS 2.0 Score = 9.3**

The RPC implementation in the server in Novell Cloud Manager 1.1.2 before Patch 3 does not properly initialize objects, which allows remote attackers to execute arbitrary code by making RPC calls that leverage incorrect privileges associated with a partially initialized session.

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

**References:**

MISC: <http://zerodayinitiative.com/advisories/ZDI-11-278/>

BID: <http://www.securityfocus.com/bid/49432>

SECUNIA: <http://secunia.com/advisories/45845>

CONFIRM: <http://download.novell.com/Download?buildid=NSONIV5PqMo~>

**CVE Reference:** [CVE-2011-2654](#)

• **CVE-2011-2184 Linux CVSS 2.0 Score = 7.2**

The key\_replace\_session\_keyring function in security/keys/process\_keys.c in the Linux kernel before 2.6.39.1 does not initialize a certain structure member, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via a KEYCTL\_SESSION\_TO\_PARENT argument to the keyctl function, a different vulnerability than CVE-2010-2960. Per: <http://cwe.mitre.org/data/definitions/476.html> 'CWE-476: NULL Pointer Dereference'

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

**References:**

MLIST: <https://lkml.org/lkml/2011/5/25/265>

MLIST: <http://www.openwall.com/lists/oss-security/2011/06/06/2>

MLIST: <http://www.openwall.com/lists/oss-security/2011/06/03/2>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=f7285b5d631fd6096b11c6af0058ed3a2b30ef4e>

MLIST: <https://lkml.org/lkml/2011/5/24/502>

MLIST: <https://lkml.org/lkml/2011/5/23/199>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39.1>

MISC: [http://alt.swiecki.net/linux\\_kernel/sys\\_open-kmem\\_cache\\_alloc-2.6.39-rc4.txt](http://alt.swiecki.net/linux_kernel/sys_open-kmem_cache_alloc-2.6.39-rc4.txt)

**CVE Reference:** [CVE-2011-2184](#)

• **CVE-2011-2723 Linux CVSS 2.0 Score = 5.7**

The skb\_gro\_header\_slow function in include/linux/netdevice.h in the Linux kernel before 2.6.39.4, when Generic Receive Offload (GRO) is enabled, resets certain fields in incorrect situations, which allows remote attackers to cause a denial of service (system crash) via crafted network traffic.

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

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=726552](https://bugzilla.redhat.com/show_bug.cgi?id=726552)

MLIST: <http://openwall.com/lists/oss-security/2011/07/29/1>

MLIST: <http://openwall.com/lists/oss-security/2011/07/28/13>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=17dd759c67f21e34f2156abcf415e1f60605a188>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39.4>

SECTRAK: <http://securitytracker.com/id?1025876>

**CVE Reference:** [CVE-2011-2723](#)

• **CVE-2011-1776 Linux CVSS 2.0 Score = 5.6**

The is\_gpt\_valid function in fs/partitions/efi.c in the Linux kernel before 2.6.39 does not check the size of an Extensible Firmware Interface (EFI) GUID Partition Table (GPT) entry, which allows physically proximate attackers to cause a denial of service (heap-based buffer overflow and OOPS) or obtain sensitive information from kernel heap memory by connecting a crafted GPT storage device, a different vulnerability than CVE-2011-1577.

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

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=703026](https://bugzilla.redhat.com/show_bug.cgi?id=703026)

MLIST: <http://openwall.com/lists/oss-security/2011/05/10/4>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=fa039d5f6b126fd65eefa05db2f67e44df8f121>

BID: <http://www.securityfocus.com/bid/47796>

MISC: <http://www.pre-cert.de/advisories/PRE-SA-2011-04.txt>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39>

**CVE Reference:** [CVE-2011-1776](#)

• **CVE-2011-1771 Linux CVSS 2.0 Score = 4.7**

The cifs\_close function in fs/cifs/file.c in the Linux kernel before 2.6.39 allows local users to cause a denial of service (NULL pointer dereference and BUG) or possibly have unspecified other impact by setting the O\_DIRECT flag during an attempt to open a file on a CIFS filesystem. Per: <http://cwe.mitre.org/data/definitions/476.html> 'CWE-476: NULL Pointer Dereference'

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

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=703016](https://bugzilla.redhat.com/show_bug.cgi?id=703016)

MLIST: <http://www.openwall.com/lists/oss-security/2011/05/09/2>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=7797069305d13252fd66cf722aa8f2cbeb3c95cd>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39>

MLIST: <http://marc.info/?l=linux-cifs&m=130204730006155&w=2>

MLIST: <http://marc.info/?l=linux-cifs&m=130204357001849&w=2>

**CVE Reference:** [CVE-2011-1771](#)

**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)