

## 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

[CodeRed Worm Scanner](#) - The S4 CodeRed Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any have been infected by CodeRed Worm.

Download Here:

<http://www.netvigilance.com/productdownloads?productname=coderedwormscanner>

## This Week in Review

Shortened url's the new weapon for spammers. Data Loss Products not good enough. Attacks that could have been prevented. New automated encryption upgrade not authorized by Mastercard.

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

### • Spammers exploiting trust in shortened URLs

The amount of spam containing shortened URLs has drastically increased recently, according to the latest statistics from Symantec.

Previously, shortened URLs -- miniature links swapped out for longer, original addresses -- were used in about 0.3 to 0.4 percent of all spam, Matt Sergeant, senior anti-spam technologist at Symantec's MessageLabs, told SCMagazineUS.com on Tuesday. During the middle of last week, however, junk mail containing the shortened links jumped to two percent of all spam.

The URLs mostly are part of spam campaigns for weight loss or male enhancement drugs, Sergeant said. If a user clicks the link in the spam, they are directed to sites that offer the products that spammers are advertising. Currently, these sites do not contain malware, but there's nothing stopping spammers from using malicious links in the future to expand the size of their botnets and the number of machines they control. SC Magazine

Full Story :

<http://www.scmagazineus.com/Spammers-exploiting-trust-in-shortened-URLs/article/139716/>

## • Solving the DLP Puzzle: 5 Technologies That Will Help

CSO - About this series: Companies are clamoring for Data Loss Prevention (DLP) tools to keep their data safe from online predators. But there is much confusion over what the true ingredients are. In this series, CSOnline talks to security practitioners, analysts and other experts for a crash-course on what DLP is, what it isn't and how to get on the right track. We'll begin with the proper technologies to use, followed by the right people policies.

Most security vendors will tell you they have just the thing for your DLP needs. But some industry experts say enterprises often buy products that, once installed, don't perform all the functions necessary to keep sensitive information safe. [See also: Security Analyst to DLP Vendors: Watch Your Language] Computerworld

Full Story :

[http://www.computerworld.com/s/article/9135299/Solving\\_the\\_DLP\\_Puzzle\\_5\\_Technologies\\_That\\_Will\\_Help?source=](http://www.computerworld.com/s/article/9135299/Solving_the_DLP_Puzzle_5_Technologies_That_Will_Help?source=)

## • Stopping cyber attacks: When are we going to learn?

CareerJournal - The latest DDOS attack demonstrates that there can be major damage from completely preventable attacks. I explained how such attacks are preventable two and a half years ago. Nonetheless, I woke up yesterday morning to the news that U.S. government Web sites are being bombarded by a massive DDOS attack. Actually, the attacks had been going on for four days, but it wasn't reported until Wednesday. It appears that this offensive involves a variant of the MyDoom attack that was first identified in 2004. While the media claims that this is "a highly sophisticated" and coordinated attack, the fact is that it is hit-or-miss; unfortunately, the state of Internet security pretty much guarantees it will hit. The way MyDoom variant attacks work is that the virus infects a vulnerable system and then 1) the system begins to bombard the targeted sites and 2) sends out malicious e-mail messages to other computers. The malicious e-mails will then infect other vulnerable systems. Just think of this as the Conficker worm with a malicious payload. The key phrase is "vulnerable systems." Antivirus product vendors have likely already posted updates to prevent the spread of this attack. However, given that a significant percentage of systems on the Internet aren't properly protected, this attack will continue for a long time to come. There is nothing sophisticated about it. It is essentially a brute force attack that keeps trying until it is specifically stopped or it runs out of vulnerable systems. Brute force is not sophisticated. While this attack seems to be causing major problems, it is so far more of a nuisance than a problem. It does however indicate potential attacks to come. In February 2007, I wrote a column in Computerworld recommending four laws that need to be passed to mitigate botnets and the like, which would include the current attack. The laws basically would require ISPs to filter out clear attack traffic and cut potential botnets off of their network. It is far easier for an ISP to stop a dozen malicious connections originating on its network than for targeted sites to stop tens of thousands of connections from hundreds of ISPs. The ISPs are being used as conduits of crime, reason enough to take seriously the recommendations I made two and a half years ago. Some critics may object that my proposed laws would only apply to U.S. systems, while the attacks are international in nature. But the fact is that if ISPs are responsible for filtering the attacks as they enter the U.S., then the attacks won't reach their targets, no matter where they originate. In any case, a very large portion of bots, if not most bots, are still in the U.S. 1 2 Next » Computerworld

Full Story :

[http://www.computerworld.com/s/article/9135336/Stopping\\_cyber\\_attacks\\_When\\_are\\_we\\_going\\_to\\_learn\\_?source=](http://www.computerworld.com/s/article/9135336/Stopping_cyber_attacks_When_are_we_going_to_learn_?source=)

## • MasterCard will not permit automated encryption upgrade

MasterCard is not allowing merchants to make use of new technology that would automate the process of upgrading encryption keys on certain point-of-sale (POS) systems, a Gartner analyst said.

The technology is called remote key injection (RKI) and enables merchants to install new encryption keys electronically, instead of having to do it manually. Avivah Litan, vice president and distinguished analyst at Gartner, told SCMagazineUS.com on Thursday that a number of her clients said MasterCard will not allow the technology.

"It could be that MasterCard found a valid security problem with it, but they are not saying anything," Litan said. SC Magazine

Full Story :

<http://www.scmagazineus.com/MasterCard-will-not-permit-automated-encryption-upgrade/article/139803/>

## New Vulnerabilities Tested in SecureScout

### • 14063 Samba Uninitialized read of a data value Vulnerability

The smbd daemon in Samba 3.0.31 - 3.3.5 contains an uninitialized read of a data value that can potentially affect access control. If a user is trying to modify an access control list (ACL) and is denied permission, this deny may be overridden if the parameter "dos filemode" is set to "yes" in the smb.conf and the user already has write access to the file. The error occurs in checking that the user has write access. Uninitialized memory is read instead of the values in the 'stat' struct of the file.

An attack would be difficult to script by an attacker, as the attacker would need to find a reproducible case to ensure previously used stack memory had the correct values to trigger the bug. In addition, the server would have to have been configured with "dos filemode = yes" in the smb.conf.

The issue has been fixed in Samba version 3.2.13, 3.0.35, and 3.3.6.

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

#### References:

- \* CONFIRM:  
<http://www.samba.org/samba/ftp/patches/security/samba-3.0.34-CVE-2009-1888.patch>
- \* CONFIRM:  
<http://www.samba.org/samba/ftp/patches/security/samba-3.2.12-CVE-2009-1888.patch>
- \* CONFIRM:  
<http://www.samba.org/samba/ftp/patches/security/samba-3.3.5-CVE-2009-1888.patch>
- \* CONFIRM:  
<http://www.samba.org/samba/security/CVE-2009-1888.html>
- \* BID: 35472  
<http://www.securityfocus.com/bid/35472>
- \* SECTRACK: 1022442  
<http://www.securitytracker.com/id?1022442>
- \* SECUNIA: 35539  
<http://secunia.com/advisories/35539>
- \* VUPEN: ADV-2009-1664  
<http://www.vupen.com/english/advisories/2009/1664>

#### CVE Reference:

CVE-2009-1888 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 14064 Samba Formatstring vulnerability in smbclient

The smbclient utility in Samba 3.2.0 - 3.2.12 contains a formatstring vulnerability where commands dealing with file names treat user input as format strings to asprintf.

An example is:

```
smb: \> put aa%3Fbb
putting file aa%3Fbb as \aa0,000000bb (0,0 kb/s) (average 0,0 kb/s)
```

As is obvious, "aa%3Fbb" is interpreted as a format string. With a maliciously crafted file name smbclient can be made to execute code triggered by the server.

The attack from our point of view is rather unlikely because the malicious filename has to be entered by the user. If smbclient is used within scripts, an attack becomes possible.

The issue has been fixed in Samba version 3.2.13.

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

#### References:

- \* CONFIRM:  
<http://www.samba.org/samba/ftp/patches/security/samba-3.2.12-CVE-2009-1886.patch>
- \* CONFIRM:  
<http://www.samba.org/samba/security/CVE-2009-1886.html>
- \* CONFIRM:  
[https://bugzilla.samba.org/show\\_bug.cgi?id=6478](https://bugzilla.samba.org/show_bug.cgi?id=6478)
- \* BID: 35472  
<http://www.securityfocus.com/bid/35472>
- \* SECTRACK: 1022441  
<http://www.securitytracker.com/id?1022441>
- \* SECUNIA: 35539  
<http://secunia.com/advisories/35539>
- \* VUPEN: ADV-2009-1664  
<http://www.vupen.com/english/advisories/2009/1664>

#### CVE Reference:

CVE-2009-1886 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 14065 Samba Potential access to "/" Vulnerability

When connecting to a share called "" (empty string) using an older version of smbclient (before 3.0.28) for example with:

```
'smbclient //server/ -U user%pass'
```

access to the root filesystem is granted with the privileges of the authenticated user. This only happens in setups with registry shares enabled by setting "registry shares = yes" which is implicitly set with "include = registry" and "config backend = registry", but is not the default.

The issue has been fixed in Samba version 3.2.7.

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

#### References:

\* MISC:

<http://master.samba.org/samba/ftp/patches/security/samba-3.2.6-CVE-2009-0022.patch>

\* CONFIRM:

<http://www.samba.org/samba/security/CVE-2009-0022.html>

\* FEDORA: FEDORA-2009-0268

<https://www.redhat.com/archives/fedora-package-announce/2009-January/msg00309.html>

\* MANDRIVA: MDVSA-2009:042

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:042>

\* UBUNTU: USN-702-1

<http://www.ubuntu.com/support/documentation/usn/usn-702-1>

\* BID: 33118

<http://www.securityfocus.com/bid/33118>

\* SECTRAK: 1021513

<http://www.securitytracker.com/id?1021513>

\* SECUNIA: 33392

<http://secunia.com/advisories/33392>

\* VUPEN: ADV-2009-0017

<http://www.frsirt.com/english/advisories/2009/0017>

\* OSVDB: 51152

<http://osvdb.org/51152>

\* SECUNIA: 33379

<http://secunia.com/advisories/33379>

\* SECUNIA: 33431

<http://secunia.com/advisories/33431>

\* XF: samba-file-system-security-bypass(47733)

<http://xforce.iss.net/xforce/xfdb/47733>

#### CVE Reference:

CVE-2009-0022 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### ● 14066 Samba Potential leak of arbitrary memory contents Vulnerability

Samba 3.0.29 and beyond contain a change to deal with gcc 4 optimizations. Part of the change modified range checking for client-generated offsets of secondary trans, trans2 and ntrans requests. These requests are used to transfer arbitrary amounts of memory from clients to servers and back using small SMB requests and contain two offsets: One offset (A) pointing into the PDU sent by the client and one (B) to direct the transferred contents into the buffer built on the server side. While the range checking for offset (B) is correct, a cut&paste error lets offset (A) pass completely unchecked against overflow.

The buffers passed into trans, trans2 and ntrans undergo higher-level processing like DCE/RPC requests or listing directories. The missing bounds check means that a malicious client can make the server do this higher-level processing on arbitrary memory contents of the smbd process handling the request. It is unknown if that can be abused to pass arbitrary memory contents back to the client, but an important barrier is missing from the affected Samba versions.

The issue has been fixed in Samba versions 3.2.5 and 3.0.33.

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

#### References:

\* CONFIRM:

<http://us1.samba.org/samba/ftp/patches/security/samba-3.0.32-CVE-2008-4314.patch>

\* CONFIRM:

<http://us1.samba.org/samba/security/CVE-2008-4314.html>

\* FEDORA: FEDORA-2008-10518

<http://www.redhat.com/archives/fedora-package-announce/2008-December/msg00021.html>  
\* FEDORA: FEDORA-2008-10638  
<http://www.redhat.com/archives/fedora-package-announce/2008-December/msg00141.html>  
\* SLACKWARE: SSA:2008-333-01  
<http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.453684>  
\* SUNALERT: 249087  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-249087-1>  
\* SUSE: SUSE-SR:2008:027  
<http://lists.opensuse.org/opensuse-security-announce/2008-12/msg00002.html>  
\* UBUNTU: USN-680-1  
<http://www.ubuntu.com/usn/USN-680-1>  
\* BID: 32494  
<http://www.securityfocus.com/bid/32494>  
\* VUPEN: ADV-2008-3277  
<http://www.frsirt.com/english/advisories/2008/3277>  
\* VUPEN: ADV-2009-0067  
<http://www.frsirt.com/english/advisories/2009/0067>  
\* OSVDB: 50230  
<http://osvdb.org/50230>  
\* SECTRAK: 1021287  
<http://www.securitytracker.com/id?1021287>  
\* SECUNIA: 32813  
<http://secunia.com/advisories/32813>  
\* SECUNIA: 32919  
<http://secunia.com/advisories/32919>  
\* SECUNIA: 32951  
<http://secunia.com/advisories/32951>  
\* SECUNIA: 32968  
<http://secunia.com/advisories/32968>

#### CVE Reference:

CVE-2008-4314 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 14513 Adobe Acrobat / Reader Heap-based buffer overflow in the JBIG2 filter Vulnerability (CVE-2009-0509) (Remote File Checking)

Heap-based buffer overflow in the JBIG2 filter in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 allows remote attackers to execute arbitrary code via a crafted file that triggers memory corruption.

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

#### References:

\* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb09-07.html>  
\* REDHAT: RHSA-2009:1109  
<http://www.redhat.com/support/errata/RHSA-2009-1109.html>  
\* SUSE: SUSE-SR:2009:012  
<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>  
\* CERT: TA09-161A  
<http://www.us-cert.gov/cas/techalerts/TA09-161A.html>  
\* BID: 35274  
<http://www.securityfocus.com/bid/35274>  
\* SECTRAK: 1022361  
<http://securitytracker.com/id?1022361>  
\* SECUNIA: 34580  
<http://secunia.com/advisories/34580>  
\* SECUNIA: 35496  
<http://secunia.com/advisories/35496>  
\* VUPEN: ADV-2009-1547  
<http://www.vupen.com/english/advisories/2009/1547>  
\* XF: reader-text-bo(49239)  
<http://xforce.iss.net/xforce/xfdb/49239>

#### CVE Reference:

CVE-2009-0509 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 14514 Adobe Acrobat / Reader Heap-based buffer overflow in the JBIG2 filter Vulnerability (CVE-2009-0510) (Remote File Checking)

Heap-based buffer overflow in the JBIG2 filter in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-0511, CVE-2009-0512, CVE-2009-0888, and CVE-2009-0889.

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

#### References:

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb09-07.html>
- \* REDHAT: RHSA-2009:1109  
<http://www.redhat.com/support/errata/RHSA-2009-1109.html>
- \* SUSE: SUSE-SR:2009:012  
<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>
- \* CERT: TA09-161A  
<http://www.us-cert.gov/cas/techalerts/TA09-161A.html>
- \* BID: 35274  
<http://www.securityfocus.com/bid/35274>
- \* SECTRACK: 1022361  
<http://securitytracker.com/id?1022361>
- \* SECUNIA: 34580  
<http://secunia.com/advisories/34580>
- \* SECUNIA: 35496  
<http://secunia.com/advisories/35496>
- \* VUPEN: ADV-2009-1547  
<http://www.vupen.com/english/advisories/2009/1547>

#### CVE Reference:

CVE-2009-0510 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 14515 Adobe Acrobat / Reader Heap-based buffer overflow in the JBIG2 filter Vulnerability (CVE-2009-0511) (Remote File Checking)

Heap-based buffer overflow in the JBIG2 filter in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-0510, CVE-2009-0512, CVE-2009-0888, and CVE-2009-0889.

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

#### References:

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb09-07.html>
- \* REDHAT: RHSA-2009:1109  
<http://www.redhat.com/support/errata/RHSA-2009-1109.html>
- \* SUSE: SUSE-SR:2009:012  
<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>
- \* CERT: TA09-161A  
<http://www.us-cert.gov/cas/techalerts/TA09-161A.html>
- \* BID: 35274  
<http://www.securityfocus.com/bid/35274>
- \* SECTRACK: 1022361  
<http://securitytracker.com/id?1022361>
- \* SECUNIA: 34580  
<http://secunia.com/advisories/34580>
- \* SECUNIA: 35496  
<http://secunia.com/advisories/35496>
- \* VUPEN: ADV-2009-1547  
<http://www.vupen.com/english/advisories/2009/1547>

#### CVE Reference:

CVE-2009-0511 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 14516 Adobe Acrobat / Reader Heap-based buffer overflow in the JBIG2 filter Vulnerability (CVE-2009-0512) (Remote File Checking)

Heap-based buffer overflow in the JBIG2 filter in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-0510, CVE-2009-0511,

CVE-2009-0888, and CVE-2009-0889.

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

#### References:

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb09-07.html>
- \* REDHAT: RHSA-2009:1109  
<http://www.redhat.com/support/errata/RHSA-2009-1109.html>
- \* SUSE: SUSE-SR:2009:012  
<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>
- \* CERT: TA09-161A  
<http://www.us-cert.gov/cas/techalerts/TA09-161A.html>
- \* BID: 35274  
<http://www.securityfocus.com/bid/35274>
- \* BID: 35293  
<http://www.securityfocus.com/bid/35293>
- \* SECTRACK: 1022361  
<http://securitytracker.com/id?1022361>
- \* SECUNIA: 34580  
<http://secunia.com/advisories/34580>
- \* SECUNIA: 35496  
<http://secunia.com/advisories/35496>
- \* VUPEN: ADV-2009-1547  
<http://www.vupen.com/english/advisories/2009/1547>

#### CVE Reference:

CVE-2009-0512 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 14517 Adobe Acrobat / Reader Heap-based buffer overflow in the JBIG2 filter Vulnerability (CVE-2009-0888) (Remote File Checking)

Heap-based buffer overflow in the JBIG2 filter in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-0510, CVE-2009-0511, CVE-2009-0512, and CVE-2009-0889.

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

#### References:

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb09-07.html>
- \* REDHAT: RHSA-2009:1109  
<http://www.redhat.com/support/errata/RHSA-2009-1109.html>
- \* CERT: TA09-161A  
<http://www.us-cert.gov/cas/techalerts/TA09-161A.html>
- \* BID: 35274  
<http://www.securityfocus.com/bid/35274>
- \* SECTRACK: 1022361  
<http://securitytracker.com/id?1022361>
- \* SECUNIA: 34580  
<http://secunia.com/advisories/34580>
- \* SECUNIA: 35496  
<http://secunia.com/advisories/35496>
- \* VUPEN: ADV-2009-1547  
<http://www.vupen.com/english/advisories/2009/1547>

#### CVE Reference:

CVE-2009-0888 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 14754 Mozilla Firefox file upload controls, upload arbitrary files Vulnerability (CVE-2006-2782) (Remote File Checking)

A vulnerability has been reported in Firefox.

An error in the handling of file upload controls can be exploited to upload arbitrary files from a user's system by e.g. dynamically changing a text input box to a file upload control.

The vulnerability has been reported in version 1.5 up to 1.5.4 not included.

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

## References:

- \* BUGTRAQ: 20060602 rPSA-2006-0091-1 firefox thunderbird  
<http://www.securityfocus.com/archive/1/archive/1/435795/100/0/threaded>
- \* CONFIRM:  
<http://www.mozilla.org/security/announce/2006/mfsa2006-41.html>
- \* DEBIAN: DSA-1118  
<http://www.debian.org/security/2006/dsa-1118>
- \* DEBIAN: DSA-1120  
<http://www.debian.org/security/2006/dsa-1120>
- \* DEBIAN: DSA-1134  
<http://www.debian.org/security/2006/dsa-1134>
- \* GENTOO: GLSA-200606-12  
<http://www.gentoo.org/security/en/glsa/glsa-200606-12.xml>
- \* HP: HPSBUX02153  
<http://www.securityfocus.com/archive/1/archive/1/446658/100/200/threaded>
- \* MANDRIVA: MDKSA-2006:143  
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:143>
- \* MANDRIVA: MDKSA-2006:145  
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:145>
- \* REDHAT: RHSA-2006:0578  
<http://www.redhat.com/support/errata/RHSA-2006-0578.html>
- \* REDHAT: RHSA-2006:0610  
<http://www.redhat.com/support/errata/RHSA-2006-0610.html>
- \* REDHAT: RHSA-2006:0611  
<http://www.redhat.com/support/errata/RHSA-2006-0611.html>
- \* REDHAT: RHSA-2006:0609  
<http://rhn.redhat.com/errata/RHSA-2006-0609.html>
- \* REDHAT: RHSA-2006:0594  
<http://www.redhat.com/support/errata/RHSA-2006-0594.html>
- \* SUSE: SUSE-SA:2006:035  
[http://www.novell.com/linux/security/advisories/2006\\_35\\_mozilla.html](http://www.novell.com/linux/security/advisories/2006_35_mozilla.html)
- \* UBUNTU: USN-296-1  
<http://www.ubuntulinux.org/support/documentation/usn/usn-296-1>
- \* UBUNTU: USN-296-2  
<http://www.ubuntulinux.org/support/documentation/usn/usn-296-2>
- \* UBUNTU: USN-323-1  
<http://www.ubuntulinux.org/support/documentation/usn/usn-323-1>
- \* BID: 18228  
<http://www.securityfocus.com/bid/18228>
- \* VUPEN: ADV-2006-2106  
<http://www.frsirt.com/english/advisories/2006/2106>
- \* VUPEN: ADV-2006-3748  
<http://www.frsirt.com/english/advisories/2006/3748>
- \* VUPEN: ADV-2008-0083  
<http://www.frsirt.com/english/advisories/2008/0083>
- \* SECTRACK: 1016202  
<http://securitytracker.com/id?1016202>
- \* SECUNIA: 20376  
<http://secunia.com/advisories/20376>
- \* SECUNIA: 20561  
<http://secunia.com/advisories/20561>
- \* SECUNIA: 21134  
<http://secunia.com/advisories/21134>
- \* SECUNIA: 21183  
<http://secunia.com/advisories/21183>
- \* SECUNIA: 21176  
<http://secunia.com/advisories/21176>
- \* SECUNIA: 21178  
<http://secunia.com/advisories/21178>
- \* SECUNIA: 21188  
<http://secunia.com/advisories/21188>
- \* SECUNIA: 21269  
<http://secunia.com/advisories/21269>
- \* SECUNIA: 21270  
<http://secunia.com/advisories/21270>
- \* SECUNIA: 21336

<http://secunia.com/advisories/21336>

\* SECUNIA: 21324

<http://secunia.com/advisories/21324>

\* SECUNIA: 21532

<http://secunia.com/advisories/21532>

\* SECUNIA: 21631

<http://secunia.com/advisories/21631>

\* SECUNIA: 22066

<http://secunia.com/advisories/22066>

\* XF: mozilla-firefox-textbox-file-access(26851)

<http://xforce.iss.net/xforce/xfdb/26851>

#### CVE Reference:

CVE-2006-2782 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

### • CVE-2008-0015 Microsoft CVSS 2.0 Score = 9.3

Stack-based buffer overflow in MPEG2TuneRequest in the Microsoft Video ActiveX control in msvidctl.dll in Microsoft DirectShow in Windows 2000, XP, and Server 2003 allows remote attackers to execute arbitrary code via a crafted web page, as exploited in the wild in July 2009.

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

#### References:

BID: <http://www.securityfocus.com/bid/35558>

CONFIRM: <http://www.microsoft.com/technet/security/advisory/972890.msp>

ISS: <http://www.iss.net/threats/329.html>

MISC: <http://www.csis.dk/dk/nyheder/nyheder.asp?tekstID=799>

MISC: <http://isc.sans.org/diary.html?storyid=6733>

CVE Reference: [CVE-2008-0015](http://cve.mitre.org/cve/2008/0015)

### • CVE-2008-0020 Microsoft CVSS 2.0 Score = 9.3

Unspecified vulnerability in the Microsoft Video ActiveX control in msvidctl.dll allows remote attackers to execute arbitrary code via unknown vectors that trigger memory corruption, a different vulnerability than CVE-2008-0015.

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

#### References:

ISS: <http://www.iss.net/threats/329.html>

CVE Reference: [CVE-2008-0020](http://cve.mitre.org/cve/2008/0020)

### • CVE-2009-2350 Microsoft CVSS 2.0 Score = 4.3

Microsoft Internet Explorer 6.0.2900.2180 and earlier does not block javascript: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header or (2) specifying the content of a Refresh header, a related issue to CVE-2009-1312.

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

#### References:

BID: <http://www.securityfocus.com/bid/35570>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/504723/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/504718/100/0/threaded>

MISC: <http://websecurity.com.ua/3275/>

CVE Reference: [CVE-2009-2350](http://cve.mitre.org/cve/2009/2350)

• **CVE-2009-1890 Apache CVSS 2.0 Score = 5.0**

The stream\_reqbody\_cl function in mod\_proxy\_http.c in the mod\_proxy module in the Apache HTTP Server before 2.3.3, when a reverse proxy is configured, does not properly handle an amount of streamed data that exceeds the Content-Length value, which allows remote attackers to cause a denial of service (CPU consumption) via crafted requests.

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

**References:**

CONFIRM:

[http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod\\_proxy\\_http.c?r1=790587&r2=790586&pathrev=790587](http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_http.c?r1=790587&r2=790586&pathrev=790587)

CONFIRM: <http://svn.apache.org/viewvc?view=rev&revision=790587>

CONFIRM: <http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?revision=790587>

CONFIRM: <http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=790587&r2=790586&pathrev=790587>

SECUNIA: <http://secunia.com/advisories/35691>

**CVE Reference:** [CVE-2009-1890](#)

• **CVE-2009-0904 IBM CVSS 2.0 Score = 6.4**

The IBM Stax XMLStreamWriter in the Web Services component in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.25 does not properly process XML encoding, which allows remote attackers to bypass intended access restrictions and possibly modify data via "XML fuzzing attacks" sent through SOAP requests.

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

**References:**

XF: <http://xforce.iss.net/xforce/xfdb/51490>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27007951>

**CVE Reference:** [CVE-2009-0904](#)

• **CVE-2009-2400 PHP CVSS 2.0 Score = 7.5**

SQL injection vulnerability in the PHP (com\_php) component for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter to index.php.

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

**References:**

VUPEN: <http://www.vupen.com/english/advisories/2009/1732>

**CVE Reference:** [CVE-2009-2400](#)

• **CVE-2009-2315 Apple CVSS 2.0 Score = 10.0**

Unspecified vulnerability in Apple iPhone OS allows remote attackers to execute arbitrary code, obtain GPS coordinates, or enable the microphone via an SMS message, as demonstrated by Charlie Miller at SyScan '09 Singapore.

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

**References:**

MISC: <http://www.syscan.org/Sg/program.html>

MISC: [http://news.cnet.com/8301-1009\\_3-10278472-83.html](http://news.cnet.com/8301-1009_3-10278472-83.html)

**CVE Reference:** [CVE-2009-2315](#)

• **CVE-2009-2421 Apple CVSS 2.0 Score = 9.3**

The CFCharacterSetInitInlineBuffer method in CoreFoundation.dll in Apple Safari 3.2.3 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly execute arbitrary code via a "high-bit character" in a URL fragment for an unspecified protocol.

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

**References:**

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/504479/100/0/threaded>

**CVE Reference:** [CVE-2009-2421](#)

**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)