

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

[Sapphire Worm Scanner](#) - The S4 Sapphire Worm 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 Microsoft SQL buffer overflow vulnerability (MS02-039/MS02-061) that the recent Sapphire Worm uses to propagate.

Download Here:

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

This Week in Review

Usage of security logs increasing. Hearing questions whether PCI increases security. Pentagon spends big on security repairs. Washington waiting for cybersecurity report.

Enjoy reading & Stay safe.

Call or email netVigilance to get an update on SecureScout.

(503) 524 5758 or sales@netvigilance.com

Top Security News Stories this Week

- **SANS report shows security logs no longer "geek toys"**

Organizations use security log data to a greater extent than ever before, according to the 2009 Annual Log Management Survey from the SANS Institute.

In addition, organizations increasingly integrated log data with their security information event management (SIEM) systems, according to the survey. More than 30 percent of respondents said they are integrating log management with SIEM, and 26 percent plan to do so.

SC Magazine

Full Story :

<http://www.scmagazineus.com/SANS-report-shows-security-logs-no-longer-geek-toys/article/130321/>

• Critics tear into PCI security rules at congressional hearing

April 6, 2009 (Computerworld) At a congressional hearing last week, federal lawmakers and retail industry officials contended that the PCI security rules have done little to stop payment card data thefts and fraud.

National Retail Federation CIO David Hogan claimed that the rules — formally known as the Payment Card Industry Data Security Standard — are little more than a tool for shifting financial risks from banks and credit card companies to retailers.

This version of the story originally appeared in Computerworld's print issue. An expanded version has also been posted on our Web site.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=336833&source=rss_topic17

• Cyberattack repairs cost Pentagon \$100 million in six months

Updated Wednesday, April 8 at 5:27 p.m. EST

The Pentagon has spent more than \$100 million in the past six months repairing damage to its networks caused by cyberattacks, according to military officials.

Officials last fall began tracking the amount of money being spent in response to cyberincidents after being directed to do so by Air Force General Kevin Chilton, commander of U.S. Strategic Command.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Cyberattack-repairs-cost-Pentagon-100-million-in-six-months/article/130376/>

• What I'll be looking for in Melissa Hathaway's report on cybersecurity

April 9, 2009 (Computerworld) The big talk in Washington's cybersecurity world is Melissa Hathaway's magical 60-day review, which is supposed to recommend how U.S. government cybersecurity efforts should be pursued. The technical press and lobbyists are all abuzz over whether or not there will be a cybersecurity coordinator who reports to the president. In certain circles, this is even more gossiped about than what Michelle Obama is wearing, but frankly the discussion is even less useful. What makes it pointless is the fact that "federal cybersecurity coordinator" could describe the supposed positions already held by such luminaries as Richard Clarke, Howard Schmidt, Paul Kurtz, Amit Yoran, Andy Purdy and, of course, Rod Beckström. Some of those people worked in the White House, some didn't. Either way, these well-qualified people accomplished relatively little in the grand scheme of things. Nonetheless, all most people seem to be looking for in the forthcoming report are a title and a reporting structure. They want to know who will have authority and where that authority will derive from. I am looking for something completely different: responsibility and accountability.

Responsibility is closer to the heart of the issue. We don't just need someone who has the authority to set policies and tell people what to do. We need staffers with the necessary technical skills who are responsible for implementing those policies (and I am making a very broad leap of faith that the policies will be useful). Right now, it doesn't seem likely that those people are going to be available. Part of the reason for that is funding. After all, Beckström resigned as director of the National Computer Security Center partly because the Department of Homeland Security didn't provide the NCSC with its congressionally allocated funding. How responsible is that?

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9131366&source=rss_topic17

New Vulnerabilities Tested in SecureScout

• 18331 Mozilla Firefox - Arbitrary code execution via XUL tree element (Remote File Checking)

Security researcher Nils reported via TippingPoint's Zero Day Initiative that the XUL tree method `_moveToEdgeShift` was in some cases triggering garbage collection routines on objects which were still in use. In such cases, the browser would crash when attempting to access a previously destroyed object and this crash could be used by an attacker to run arbitrary code on a victim's computer.

The issue has been fixed in Firefox 3.0.8.

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

References:

- * BUGTRAQ: 20090330 ZDI-09-015: Mozilla Firefox XUL _moveToEdgeShift() Memory Corruption Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/502303/100/0/threaded>
- * MISC:
<http://blogs.zdnet.com/security/?p=2934>
- * MISC:
<http://blogs.zdnet.com/security/?p=2941>
- * MISC:
<http://cansecwest.com/index.html>
- * MISC:
<http://dvlabs.tippingpoint.com/blog/2009/02/25/pwn2own-2009>
- * MISC:
<http://dvlabs.tippingpoint.com/blog/2009/03/18/pwn2own-2009-day-1---safari-internet-explorer-and-firefox-taken-down-by-f>
- * MISC:
http://news.cnet.com/8301-1009_3-10199652-83.html
- * MISC:
<http://twitter.com/tippingpoint1/status/1351635812>
- * MISC:
<http://www.h-online.com/security/Pwn2Own-2009-Safari-IE-8-and-Firefox-exploited--/news/112889>
- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-09-015>
- * CONFIRM:
<http://www.mozilla.org/security/announce/2009/mfsa2009-13.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=484320
- * CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2009-113.htm>
- * DEBIAN: DSA-1756
<http://www.debian.org/security/2009/dsa-1756>
- * FEDORA: FEDORA-2009-3101
<https://www.redhat.com/archives/fedora-package-announce/2009-March/msg01077.html>
- * MANDRIVA: MDVSA-2009:084
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:084>
- * REDHAT: RHSA-2009:0397
<http://www.redhat.com/support/errata/RHSA-2009-0397.html>
- * REDHAT: RHSA-2009:0398
<http://www.redhat.com/support/errata/RHSA-2009-0398.html>
- * BID: 34181
<http://www.securityfocus.com/bid/34181>
- * OSVDB: 52896
<http://osvdb.org/52896>
- * SECTRAK: 1021878
<http://www.securitytracker.com/id?1021878>
- * SECUNIA: 34471
<http://secunia.com/advisories/34471>
- * SECUNIA: 34527
<http://secunia.com/advisories/34527>
- * SECUNIA: 34549
<http://secunia.com/advisories/34549>
- * SECUNIA: 34550
<http://secunia.com/advisories/34550>
- * NETVIGILANCE-UNKNOWN: ADV-2009-0864
<http://www.vupen.com/english/advisories/2009/0864>

CVE Reference:

CVE-2009-1044 (cve.mitre.org, nvd.nist.gov)

• 18332 Mozilla Firefox - XSL Transformation vulnerability (Remote File Checking)

Security researcher Guido Landi discovered that a XSL stylesheet could be used to crash the browser during a XSL transformation. An attacker could potentially use this crash to run arbitrary code on a victim's computer.

This vulnerability was also previously reported as a stability problem by Ubuntu community member, Andre. Ubuntu community member Michael Rooney reported Andre's findings to Mozilla, and Mozilla community member Martin helped reduce Andre's original testcase and contributed a patch to fix the vulnerability.

The issue has been fixed in Firefox 3.0.8.

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

References:

- * MISC:
<http://blogs.zdnet.com/security/?p=3013>
- * MILW0RM: 8285
<http://www.milw0rm.com/exploits/8285>
- * CONFIRM:
<http://www.mozilla.org/security/announce/2009/mfsa2009-12.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=460090
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=485217
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=485286
- * CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2009-113.htm>
- * DEBIAN: DSA-1756
<http://www.debian.org/security/2009/dsa-1756>
- * FEDORA: FEDORA-2009-3101
<https://www.redhat.com/archives/fedora-package-announce/2009-March/msg01077.html>
- * MANDRIVA: MDVSA-2009:084
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:084>
- * REDHAT: RHSA-2009:0397
<http://www.redhat.com/support/errata/RHSA-2009-0397.html>
- * REDHAT: RHSA-2009:0398
<http://www.redhat.com/support/errata/RHSA-2009-0398.html>
- * BID: 34235
<http://www.securityfocus.com/bid/34235>
- * SECTRAK: 1021939
<http://www.securitytracker.com/id?1021939>
- * SECUNIA: 34471
<http://secunia.com/advisories/34471>
- * SECUNIA: 34527
<http://secunia.com/advisories/34527>
- * SECUNIA: 34549
<http://secunia.com/advisories/34549>
- * SECUNIA: 34550
<http://secunia.com/advisories/34550>

CVE Reference:

CVE-2009-1169 (cve.mitre.org, nvd.nist.gov)

• 18333 Mozilla Firefox - Crashes with evidence of memory corruption (Layout engine crashes) (Remote File Checking)

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue also affects the 2.x branch of Firefox.

The issue has been fixed in Firefox 3.0.6.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2009/mfsa2009-01.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=331088
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=401042
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=416461
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=420697
- * CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=421839
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=422283
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=422301
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=431705
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=437142
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=449006
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=461027
* CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2009-040.htm>
* FEDORA: FEDORA-2009-1399
<https://www.redhat.com/archives/fedora-package-announce/2009-February/msg00240.html>
* FEDORA: FEDORA-2009-2882
<https://www.redhat.com/archives/fedora-package-announce/2009-March/msg00769.html>
* FEDORA: FEDORA-2009-2884
<https://www.redhat.com/archives/fedora-package-announce/2009-March/msg00771.html>
* FEDORA: FEDORA-2009-3101
<https://www.redhat.com/archives/fedora-package-announce/2009-March/msg01077.html>
* MANDRIVA: MDVSA-2009:044
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:044>
* MANDRIVA: MDVSA-2009:083
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:083>
* REDHAT: RHSA-2009:0256
<http://rhn.redhat.com/errata/RHSA-2009-0256.html>
* REDHAT: RHSA-2009:0257
<http://www.redhat.com/support/errata/RHSA-2009-0257.html>
* REDHAT: RHSA-2009:0258
<http://www.redhat.com/support/errata/RHSA-2009-0258.html>
* SLACKWARE: SSA:2009-083-02
<http://slackware.com/security/viewer.php?l=slackware-security&y=2009&m=slackware-security.405420>
* SLACKWARE: SSA:2009-083-03
<http://slackware.com/security/viewer.php?l=slackware-security&y=2009&m=slackware-security.433952>
* UBUNTU: USN-717-1
<http://www.ubuntu.com/usn/usn-717-1>
* UBUNTU: USN-741-1
<http://www.ubuntulinux.org/support/documentation/usn/usn-741-1>
* BID: 33598
<http://www.securityfocus.com/bid/33598>
* SECUNIA: 33802
<http://secunia.com/advisories/33802>
* SECUNIA: 33831
<http://secunia.com/advisories/33831>
* SECUNIA: 33841
<http://secunia.com/advisories/33841>
* SECUNIA: 33846
<http://secunia.com/advisories/33846>
* SECUNIA: 34387
<http://secunia.com/advisories/34387>
* SECUNIA: 34324
<http://secunia.com/advisories/34324>
* SECUNIA: 34417
<http://secunia.com/advisories/34417>
* SECUNIA: 34462
<http://secunia.com/advisories/34462>
* SECUNIA: 34464
<http://secunia.com/advisories/34464>
* SECUNIA: 34527
<http://secunia.com/advisories/34527>
* NETVIGILANCE-UNKNOWN: ADV-2009-0313
<http://www.frsirt.com/english/advisories/2009/0313>
* SECTRAK: 1021663
<http://www.securitytracker.com/id?1021663>
* SECUNIA: 33799
<http://secunia.com/advisories/33799>

* SECUNIA: 33808
<http://secunia.com/advisories/33808>
* SECUNIA: 33809
<http://secunia.com/advisories/33809>
* SECUNIA: 33816
<http://secunia.com/advisories/33816>
* SECUNIA: 33869
<http://secunia.com/advisories/33869>

CVE Reference:

CVE-2009-0352 (cve.mitre.org, nvd.nist.gov)

• 18334 Mozilla Thunderbird - Crashes with evidence of memory corruption (Layout engine crashes) (Remote File Checking)

Mozilla developers identified and fixed several stability bugs in the browser engine used in Thunderbird and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue has been fixed in Thunderbird 2.0.0.21.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2009/mfsa2009-01.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=331088
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=401042
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=416461
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=420697
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=421839
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=422283
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=422301
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=431705
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=437142
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=449006
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=461027
* CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2009-040.htm>
* FEDORA: FEDORA-2009-1399
<https://www.redhat.com/archives/fedora-package-announce/2009-February/msg00240.html>
* FEDORA: FEDORA-2009-2882
<https://www.redhat.com/archives/fedora-package-announce/2009-March/msg00769.html>
* FEDORA: FEDORA-2009-2884
<https://www.redhat.com/archives/fedora-package-announce/2009-March/msg00771.html>
* FEDORA: FEDORA-2009-3101
<https://www.redhat.com/archives/fedora-package-announce/2009-March/msg01077.html>
* MANDRIVA: MDVSA-2009:044
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:044>
* MANDRIVA: MDVSA-2009:083
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:083>
* REDHAT: RHSA-2009:0256
<http://rhn.redhat.com/errata/RHSA-2009-0256.html>
* REDHAT: RHSA-2009:0257
<http://www.redhat.com/support/errata/RHSA-2009-0257.html>
* REDHAT: RHSA-2009:0258
<http://www.redhat.com/support/errata/RHSA-2009-0258.html>
* SLACKWARE: SSA:2009-083-02

<http://slackware.com/security/viewer.php?l=slackware-security&y=2009&m=slackware-security.405420>

* SLACKWARE: SSA:2009-083-03

<http://slackware.com/security/viewer.php?l=slackware-security&y=2009&m=slackware-security.433952>

* UBUNTU: USN-717-1

<http://www.ubuntu.com/usn/usn-717-1>

* UBUNTU: USN-741-1

<http://www.ubuntulinux.org/support/documentation/usn/usn-741-1>

* BID: 33598

<http://www.securityfocus.com/bid/33598>

* SECUNIA: 33802

<http://secunia.com/advisories/33802>

* SECUNIA: 33831

<http://secunia.com/advisories/33831>

* SECUNIA: 33841

<http://secunia.com/advisories/33841>

* SECUNIA: 33846

<http://secunia.com/advisories/33846>

* SECUNIA: 34387

<http://secunia.com/advisories/34387>

* SECUNIA: 34324

<http://secunia.com/advisories/34324>

* SECUNIA: 34417

<http://secunia.com/advisories/34417>

* SECUNIA: 34462

<http://secunia.com/advisories/34462>

* SECUNIA: 34464

<http://secunia.com/advisories/34464>

* SECUNIA: 34527

<http://secunia.com/advisories/34527>

* NETVIGILANCE-UNKNOWN: ADV-2009-0313

<http://www.frsirt.com/english/advisories/2009/0313>

* SECTRAK: 1021663

<http://www.securitytracker.com/id?1021663>

* SECUNIA: 33799

<http://secunia.com/advisories/33799>

* SECUNIA: 33808

<http://secunia.com/advisories/33808>

* SECUNIA: 33809

<http://secunia.com/advisories/33809>

* SECUNIA: 33816

<http://secunia.com/advisories/33816>

* SECUNIA: 33869

<http://secunia.com/advisories/33869>

CVE Reference:

CVE-2009-0352 (cve.mitre.org, nvd.nist.gov)

• 18335 Mozilla Thunderbird - Crashes with evidence of memory corruption (JavaScript engine crash) (Remote File Checking)

Mozilla developers identified and fixed several stability bugs in the browser engine used in Thunderbird and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue has been fixed in Thunderbird 2.0.0.21.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2009/mfsa2009-01.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=452913

* CONFIRM:

<http://support.avaya.com/elmodocs2/security/ASA-2009-040.htm>

* FEDORA: FEDORA-2009-1399

<https://www.redhat.com/archives/fedora-package-announce/2009-February/msg00240.html>

* FEDORA: FEDORA-2009-2882

<https://www.redhat.com/archives/fedora-package-announce/2009-March/msg00769.html>

* FEDORA: FEDORA-2009-2884
<https://www.redhat.com/archives/fedora-package-announce/2009-March/msg00771.html>

* FEDORA: FEDORA-2009-3101
<https://www.redhat.com/archives/fedora-package-announce/2009-March/msg01077.html>

* MANDRIVA: MDVSA-2009:044
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:044>

* MANDRIVA: MDVSA-2009:083
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:083>

* REDHAT: RHSA-2009:0256
<http://rhn.redhat.com/errata/RHSA-2009-0256.html>

* REDHAT: RHSA-2009:0257
<http://www.redhat.com/support/errata/RHSA-2009-0257.html>

* REDHAT: RHSA-2009:0258
<http://www.redhat.com/support/errata/RHSA-2009-0258.html>

* SLACKWARE: SSA:2009-083-02
<http://slackware.com/security/viewer.php?l=slackware-security&y=2009&m=slackware-security.405420>

* SLACKWARE: SSA:2009-083-03
<http://slackware.com/security/viewer.php?l=slackware-security&y=2009&m=slackware-security.433952>

* UBUNTU: USN-717-1
<http://www.ubuntu.com/usn/usn-717-1>

* BID: 33598
<http://www.securityfocus.com/bid/33598>

* SECUNIA: 33802
<http://secunia.com/advisories/33802>

* SECUNIA: 33831
<http://secunia.com/advisories/33831>

* SECUNIA: 33841
<http://secunia.com/advisories/33841>

* SECUNIA: 33846
<http://secunia.com/advisories/33846>

* SECUNIA: 34324
<http://secunia.com/advisories/34324>

* SECUNIA: 34417
<http://secunia.com/advisories/34417>

* SECUNIA: 34462
<http://secunia.com/advisories/34462>

* SECUNIA: 34464
<http://secunia.com/advisories/34464>

* SECUNIA: 34527
<http://secunia.com/advisories/34527>

* NETVIGILANCE-UNKNOWN: ADV-2009-0313
<http://www.frsirt.com/english/advisories/2009/0313>

* SECTRACK: 1021663
<http://www.securitytracker.com/id?1021663>

* SECUNIA: 33799
<http://secunia.com/advisories/33799>

* SECUNIA: 33808
<http://secunia.com/advisories/33808>

* SECUNIA: 33809
<http://secunia.com/advisories/33809>

* SECUNIA: 33816
<http://secunia.com/advisories/33816>

* SECUNIA: 33869
<http://secunia.com/advisories/33869>

CVE Reference:

CVE-2009-0353 (cve.mitre.org, nvd.nist.gov)

• 18336 Mozilla Firefox - Crashes with evidence of memory corruption (JavaScript engine crash) (Remote File Checking)

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue does not affect the 2.x branch of Firefox.

The issue has been fixed in Firefox 3.0.6.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2009/mfsa2009-01.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=452913
- * CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2009-040.htm>
- * FEDORA: FEDORA-2009-1399
<https://www.redhat.com/archives/fedora-package-announce/2009-February/msg00240.html>
- * FEDORA: FEDORA-2009-2882
<https://www.redhat.com/archives/fedora-package-announce/2009-March/msg00769.html>
- * FEDORA: FEDORA-2009-2884
<https://www.redhat.com/archives/fedora-package-announce/2009-March/msg00771.html>
- * FEDORA: FEDORA-2009-3101
<https://www.redhat.com/archives/fedora-package-announce/2009-March/msg01077.html>
- * MANDRIVA: MDVSA-2009:044
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:044>
- * MANDRIVA: MDVSA-2009:083
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:083>
- * REDHAT: RHSA-2009:0256
<http://rhn.redhat.com/errata/RHSA-2009-0256.html>
- * REDHAT: RHSA-2009:0257
<http://www.redhat.com/support/errata/RHSA-2009-0257.html>
- * REDHAT: RHSA-2009:0258
<http://www.redhat.com/support/errata/RHSA-2009-0258.html>
- * SLACKWARE: SSA:2009-083-02
<http://slackware.com/security/viewer.php?l=slackware-security&y=2009&m=slackware-security.405420>
- * SLACKWARE: SSA:2009-083-03
<http://slackware.com/security/viewer.php?l=slackware-security&y=2009&m=slackware-security.433952>
- * UBUNTU: USN-717-1
<http://www.ubuntu.com/usn/usn-717-1>
- * BID: 33598
<http://www.securityfocus.com/bid/33598>
- * SECUNIA: 33802
<http://secunia.com/advisories/33802>
- * SECUNIA: 33831
<http://secunia.com/advisories/33831>
- * SECUNIA: 33841
<http://secunia.com/advisories/33841>
- * SECUNIA: 33846
<http://secunia.com/advisories/33846>
- * SECUNIA: 34324
<http://secunia.com/advisories/34324>
- * SECUNIA: 34417
<http://secunia.com/advisories/34417>
- * SECUNIA: 34462
<http://secunia.com/advisories/34462>
- * SECUNIA: 34464
<http://secunia.com/advisories/34464>
- * SECUNIA: 34527
<http://secunia.com/advisories/34527>
- * NETVIGILANCE-UNKNOWN: ADV-2009-0313
<http://www.frsirt.com/english/advisories/2009/0313>
- * SECTRAK: 1021663
<http://www.securitytracker.com/id?1021663>
- * SECUNIA: 33799
<http://secunia.com/advisories/33799>
- * SECUNIA: 33808
<http://secunia.com/advisories/33808>
- * SECUNIA: 33809
<http://secunia.com/advisories/33809>
- * SECUNIA: 33816
<http://secunia.com/advisories/33816>
- * SECUNIA: 33869
<http://secunia.com/advisories/33869>

CVE Reference:

CVE-2009-0353 (cve.mitre.org, nvd.nist.gov)

• 18337 Mozilla Firefox - XSS using a chrome XBL method and window.eval (Remote File Checking)

Mozilla security researcher moz_bug_r_a4 reported that a chrome XBL method can be used in conjunction with window.eval to execute arbitrary JavaScript within the context of another website, violating the same origin policy.

The issue does not affect the 2.x branch of Firefox.

The issue has been fixed in Firefox 3.0.6.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2009/mfsa2009-02.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=468581
- * CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2009-040.htm>
- * FEDORA: FEDORA-2009-1399
<https://www.redhat.com/archives/fedora-package-announce/2009-February/msg00240.html>
- * MANDRIVA: MDVSA-2009:044
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:044>
- * REDHAT: RHSA-2009:0256
<http://rhn.redhat.com/errata/RHSA-2009-0256.html>
- * UBUNTU: USN-717-1
<http://www.ubuntu.com/usn/usn-717-1>
- * BID: 33598
<http://www.securityfocus.com/bid/33598>
- * SECUNIA: 33831
<http://secunia.com/advisories/33831>
- * SECUNIA: 33841
<http://secunia.com/advisories/33841>
- * SECUNIA: 33846
<http://secunia.com/advisories/33846>
- * NETVIGILANCE-UNKNOWN: ADV-2009-0313
<http://www.frsirt.com/english/advisories/2009/0313>
- * SECTRAK: 1021664
<http://www.securitytracker.com/id?1021664>
- * SECUNIA: 33799
<http://secunia.com/advisories/33799>
- * SECUNIA: 33809
<http://secunia.com/advisories/33809>
- * SECUNIA: 33869
<http://secunia.com/advisories/33869>

CVE Reference:

CVE-2009-0354 (cve.mitre.org, nvd.nist.gov)

• 18338 Mozilla Firefox - Local file stealing with SessionStore (Remote File Checking)

Mozilla security researcher moz_bug_r_a4 reported that a form input control's type could be changed during the restoration of a closed tab. An attacker could set an input control's text value to the path of a local file whose location was known to the attacker. If the tab was then closed and the victim persuaded to re-open it, upon restoring the tab the attacker could use this vulnerability to change the input type to file. Scripts in the page could then automatically submit the form and steal the contents of the user's local file.

The issue affects the 2.x branch of Firefox.

The issue has been fixed in Firefox 3.0.6.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2009/mfsa2009-03.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=466937
- * CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2009-040.htm>

* FEDORA: FEDORA-2009-1399
<https://www.redhat.com/archives/fedora-package-announce/2009-February/msg00240.html>

* FEDORA: FEDORA-2009-2882
<https://www.redhat.com/archives/fedora-package-announce/2009-March/msg00769.html>

* FEDORA: FEDORA-2009-2884
<https://www.redhat.com/archives/fedora-package-announce/2009-March/msg00771.html>

* MANDRIVA: MDVSA-2009:044
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:044>

* REDHAT: RHSA-2009:0256
<http://rhn.redhat.com/errata/RHSA-2009-0256.html>

* REDHAT: RHSA-2009:0257
<http://www.redhat.com/support/errata/RHSA-2009-0257.html>

* REDHAT: RHSA-2009:0258
<http://www.redhat.com/support/errata/RHSA-2009-0258.html>

* UBUNTU: USN-717-1
<http://www.ubuntu.com/usn/usn-717-1>

* UBUNTU: USN-717-2
<http://www.ubuntu.com/usn/usn-717-2>

* BID: 33598
<http://www.securityfocus.com/bid/33598>

* SECUNIA: 33831
<http://secunia.com/advisories/33831>

* SECUNIA: 33841
<http://secunia.com/advisories/33841>

* SECUNIA: 33846
<http://secunia.com/advisories/33846>

* SECUNIA: 34324
<http://secunia.com/advisories/34324>

* SECUNIA: 34417
<http://secunia.com/advisories/34417>

* NETVIGILANCE-UNKNOWN: ADV-2009-0313
<http://www.frsirt.com/english/advisories/2009/0313>

* SECTRAK: 1021665
<http://www.securitytracker.com/id?1021665>

* SECUNIA: 33799
<http://secunia.com/advisories/33799>

* SECUNIA: 33808
<http://secunia.com/advisories/33808>

* SECUNIA: 33809
<http://secunia.com/advisories/33809>

* SECUNIA: 33816
<http://secunia.com/advisories/33816>

* SECUNIA: 33869
<http://secunia.com/advisories/33869>

CVE Reference:

CVE-2009-0355 (cve.mitre.org, nvd.nist.gov)

• 18339 Mozilla Firefox - Chrome privilege escalation via local .desktop files (Remote File Checking)

Mozilla security researcher Georgi Guninski reported that the fix for an earlier vulnerability reported by Liu Die Yu using local internet shortcut files to access other sites (MFSA 2008-47) could be bypassed by redirecting to a privileged about: URI such as about:plugins. If an attacker could get a victim to download two files, a malicious HTML file and a .desktop shortcut file, they could have the HTML document load a privileged chrome document via the shortcut and both documents would be treated as same origin. This vulnerability could potentially be used by an attacker to inject arbitrary code into the chrome document and execute with chrome privileges. Because this attack has relatively high complexity, the severity of this issue was determined to be moderate.

The issue affects the 2.x branch of Firefox.

The issue has been fixed in Firefox 3.0.6.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2009/mfsa2009-04.html>

* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=460425

* CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2009-040.htm>
* FEDORA: FEDORA-2009-1399
<https://www.redhat.com/archives/fedora-package-announce/2009-February/msg00240.html>
* MANDRIVA: MDVSA-2009:044
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:044>
* REDHAT: RHSA-2009:0256
<http://rhn.redhat.com/errata/RHSA-2009-0256.html>
* BID: 33598
<http://www.securityfocus.com/bid/33598>
* SECUNIA: 33831
<http://secunia.com/advisories/33831>
* SECUNIA: 33841
<http://secunia.com/advisories/33841>
* SECUNIA: 33846
<http://secunia.com/advisories/33846>
* NETVIGILANCE-UNKNOWN: ADV-2009-0313
<http://www.frsirt.com/english/advisories/2009/0313>
* SECTRAK: 1021666
<http://www.securitytracker.com/id?1021666>
* SECUNIA: 33799
<http://secunia.com/advisories/33799>
* SECUNIA: 33809
<http://secunia.com/advisories/33809>

CVE Reference:

CVE-2009-0356 (cve.mitre.org, nvd.nist.gov)

• 18340 Mozilla Firefox - XML denial of service (Remote File Checking)

The XUL parser in Mozilla Firefox 3.0.8 and earlier 3.0.x versions allows remote attackers to cause a denial of service (memory corruption) via an XML document composed of a long series of start-tags with no corresponding end-tags.

The issue does not affect the 2.x branch of Firefox.

The issue has not yet been resolved.

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

References:

* MILWORM: 8306
<http://www.milw0rm.com/exploits/8306>
* MISC:
<http://milw0rm.com/sploits/2009-Firefox-XUL-0day-PoC.rar>
* XF: firefox-xml-dos(49521)
<http://xforce.iss.net/xforce/xfdb/49521>

CVE Reference:

CVE-2009-1232 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-1275 Apache CVSS 2.0 Score = 6.8

Apache Tiles 2.1 before 2.1.2, as used in Apache Struts and other products, evaluates Expression Language (EL) expressions twice in certain circumstances, which allows remote attackers to conduct cross-site scripting (XSS) attacks or obtain sensitive information via unspecified vectors, related to the (1) tiles:putAttribute and (2) tiles:insertTemplate JSP tags.

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

References:

CONFIRM: <https://issues.apache.org/struts/browse/TILES-351>

CONFIRM:
<http://svn.apache.org/viewvc/tiles/framework/trunk/src/site/apt/security/security-bulletin-1.appt?revision=741913>

CVE Reference: [CVE-2009-1275](#)

- **CVE-2008-2025 Apache CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in Apache Struts before 1.2.9-162.31.1 on SUSE Linux Enterprise (SLE) 11, before 1.2.9-108.2 on SUSE openSUSE 10.3, before 1.2.9-198.2 on SUSE openSUSE 11.0, and before 1.2.9-162.163.2 on SUSE openSUSE 11.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors related to "insufficient quoting of parameters."

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

References:

CONFIRM: <http://download.opensuse.org/update/10.3-test/repodata/patch-struts-5872.xml>

MISC: <https://launchpad.net/bugs/cve/2008-2025>

MISC: https://bugzilla.novell.com/show_bug.cgi?id=385273

CONFIRM: <http://support.novell.com/security/cve/CVE-2008-2025.html>

SUSE: <http://lists.opensuse.org/opensuse-security-announce/2009-04/msg00003.html>

CVE Reference: [CVE-2008-2025](#)

- **CVE-2008-6682 Apache CVSS 2.0 Score = 4.3**

Multiple cross-site scripting (XSS) vulnerabilities in Apache Struts 2.0.x before 2.0.11.1 and 2.1.x before 2.1.1 allow remote attackers to inject arbitrary web script or HTML via vectors associated with improper handling of (1) " (double quote) characters in the href attribute of an s:a tag and (2) parameters in the action attribute of an s:url tag.

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

References:

CONFIRM:
<http://www.nabble.com/Feedback%3A-WW-2414%2C-XSS-attack-is-possible-if-using-%3Cs%3Aurl...%3E-and-%3Cs%3A>

CONFIRM:
<http://www.nabble.com/Feedback%3A-WW-2414%2C-XSS-attack-is-possible-if-using-%3Cs%3Aurl...%3E-and-%3Cs%3A>

CONFIRM: <https://issues.apache.org/struts/browse/WW-2427>

CONFIRM: <https://issues.apache.org/struts/browse/WW-2414>

CVE Reference: [CVE-2008-6682](#)

- **CVE-2008-5519 Apache CVSS 2.0 Score = 2.6**

The JK Connector (aka mod_jk) 1.2.0 through 1.2.26 in Apache Tomcat allows remote attackers to obtain sensitive information via an arbitrary request from an HTTP client, in opportunistic circumstances involving (1) a request from a different client that included a Content-Length header but no POST data or (2) a rapid series of requests, related to noncompliance with the AJP protocol's requirements for requests containing Content-Length headers.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=490201

BID: <http://www.securityfocus.com/bid/34412>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/502530/100/0/threaded>

CONFIRM: <http://tomcat.apache.org/security-jk.html>

CONFIRM: <http://tomcat.apache.org/connectors-doc/miscellaneous/changelog.html>

CONFIRM: <http://svn.eu.apache.org/viewvc?view=rev&revision=702540>

CONFIRM:
<http://svn.eu.apache.org/viewvc/tomcat/connectors/trunk/jk/xdocs/miscellaneous/changelog.xml?view=markup&pathrev=7>

CONFIRM:

http://svn.eu.apache.org/viewvc/tomcat/connectors/trunk/jk/native/common/jk_ajp_common.c?r1=702387&r2=702540&pathrev=702540

SECTrack: <http://securitytracker.com/id?1022001>

SECUNIA: <http://secunia.com/advisories/34621>

MLIST: <http://marc.info/?l=tomcat-dev&m=123913700700879>

MLIST:

http://mail-archives.apache.org/mod_mbox/www-announce/200904.mbox/%3C49DBBAC0.2080400@apache.org%3E

CVE Reference: [CVE-2008-5519](#)

• **CVE-2009-0796 Apache CVSS 2.0 Score = 2.6**

Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

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

References:

CONFIRM: <http://svn.apache.org/viewvc?view=rev&revision=761081>

MISC: <https://launchpad.net/bugs/cve/2009-0796>

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=494402

MLIST: <http://www.gossamer-threads.com/lists/modperl/modperl/99475#99475>

MLIST: <http://www.gossamer-threads.com/lists/modperl/modperl-cvs/99477#99477>

CONFIRM:

<http://svn.apache.org/viewvc/perl/modperl/branches/1.x/lib/Apache/Status.pm?r1=177851&r2=761081&pathrev=761081&pathrev=761081>

CVE Reference: [CVE-2009-0796](#)

• **CVE-2009-1155 Cisco CVSS 2.0 Score = 7.8**

Cisco Adaptive Security Appliances (ASA) 5500 Series and PIX Security Appliances 7.1(1) through 7.1(2)82, 7.2 before 7.2(4)27, 8.0 before 8.0(4)25, and 8.1 before 8.1(2)15, when AAA override-account-disable is entered in a general-attributes field, allow remote attackers to bypass authentication and establish a VPN session to an ASA device via unspecified vectors.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080a994f6.shtml

CVE Reference: [CVE-2009-1155](#)

• **CVE-2009-1157 Cisco CVSS 2.0 Score = 7.8**

Memory leak on Cisco Adaptive Security Appliances (ASA) 5500 Series and PIX Security Appliances 7.0 before 7.0(8)6, 7.1 before 7.1(2)82, 7.2 before 7.2(4)30, 8.0 before 8.0(4)28, and 8.1 before 8.1(2)19 allows remote attackers to cause a denial of service (memory consumption or device reload) via a crafted TCP packet.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080a994f6.shtml

CVE Reference: [CVE-2009-1157](#)

• **CVE-2009-1158 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability on Cisco Adaptive Security Appliances (ASA) 5500 Series devices 7.0 before 7.0(8)6, 7.1 before 7.1(2)82, 7.2 before 7.2(4)26, 8.0 before 8.0(4)24, and 8.1 before 8.1(2)14, when H.323 inspection is enabled, allows remote attackers to cause a denial of service (device reload) via a crafted H.323 packet.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080a994f6.shtml

CVE Reference: [CVE-2009-1158](#)

Vulnerability Resource

Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the 'security portal for information system security professionals' is well founded. <http://www.infosyssec.org/infosyssec/>

Thank You

Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at ScoutNews@netVigilance.com

About SecureScout

SecureScout is a leading vulnerability scanner and management tool developed and marketed worldwide by NexantiS Corporation.

SecureScout is a trademark of NexantiS Corporation.

netVigilance, Inc. is a partner of NexantiS and an authorized distributor of SecureScout.

For any inquiry about SecureScout by:

Customers in America and Northern Europe contact us at info@netVigilance.com

Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at info-scanner@securescout.net