

## Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

---

## Product Focus

[Apache Chunked Vulnerability Scanner](#) - The S4 Apache Chunked Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Apache Chunked Encoding buffer overflow.

Download Here:

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

## This Week in Review

Cloud safety still an issue. Another cyberspy network penetrated. ATM fraud on the rise. U.S. at risk for cyberattack.

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

### • Survey: Cloud computing risks outweigh reward

Though cloud computing is often touted as a cost-saver for companies, IT pros still have lingering doubts about the safety and security of working in the cloud.

Around 45 percent of IT professionals recently surveyed by the ISACA (formerly known as the Information Systems Audit and Control Association) said the risks involved in cloud computing outshine any benefits. A global organization focused on the auditing and security of information systems, the ISACA conducted its first annual IT Risk/Reward Barometer survey (PDF) in March.

Questioning more than 1,800 IT professionals in the U.S. who are members of the group, the ISACA found that only 10 percent of them plan to use cloud computing for mission-critical IT services, 15 percent will use it only for low-risk services, and 26 percent don't expect to tap into the cloud at all. Cnet Security

Full Story :

[http://news.cnet.com/8301-1001\\_3-20001921-92.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-1001_3-20001921-92.html?part=rss&subj=news&tag=2547-1_3-0-20)

## • U.S.-Canada research team penetrate cyberspy network

Security researchers have uncovered another sophisticated cyberespionage network that stole classified documents from a number of computer systems belonging to government agencies, businesses and other organizations.

The spying operation, dubbed Shadow Network, spread to computers in India, the United Nations and the Office of the Dalai Lama, according to a report published Monday by five researchers, four of whom are based out of the Munk School of Global Affairs at the University of Toronto. The fifth researcher, Steven Adair, is a member of the U.S.-based nonprofit Shadowserver Foundation.

Through their eight-month investigation, the researchers not only isolated infected systems - as they had done in a prior investigation known as GhostNet, which revealed some 1,300 computers that had been infected by servers that traced back to China. SC Magazine

Full Story :

[http://www.scmagazineus.com/us-canada-research-team-penetrate-cyberspy-network/article/167493/?utm\\_source=f](http://www.scmagazineus.com/us-canada-research-team-penetrate-cyberspy-network/article/167493/?utm_source=f)

## • Report: ATM fraud on the rise

Nearly one in five debit or credit card fraud victims reported having their PIN information stolen in 2009 - which represents a "considerable increase" over 2008, according to a report released Tuesday by Javelin Strategy & Research. The report, which is based on a telephone and online survey of 8,168 consumers, found that 10 percent of all fraud victims had cash withdrawn from their accounts via fraudulent ATM transactions. Twenty-three percent of those who experienced fraudulent withdrawals left their primary financial institution.

Using an ATM machine can place consumers' data at risk in several ways, according to Adam Bosnian, VP of products, strategy and sales at privileged identity management solutions vendor Cyber-Ark Software. SC Magazine

Full Story :

[http://www.scmagazineus.com/report-atm-fraud-on-the-rise/article/167613/?utm\\_source=feedburner&utm\\_medium=f](http://www.scmagazineus.com/report-atm-fraud-on-the-rise/article/167613/?utm_source=feedburner&utm_medium=f)

## • Federal IT pros say U.S. at high risk for cyberattack

Almost three-quarters of the government IT administrators polled in a new survey believe the U.S. is likely to face a cyberattack from a foreign country in the next year.

Key IT decision makers who work in national defense and security were questioned in a new Clarus Research Group survey commissioned by Lumension and released Tuesday. Among those polled for the "Federal Cyber Security Outlook for 2010 Survey," 74 percent expect a cyberattack from foreign shores in the next year.

(Credit: Lumension) Cnet Security

Full Story :

[http://news.cnet.com/8301-1009\\_3-20002009-83.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-1009_3-20002009-83.html?part=rss&subj=news&tag=2547-1_3-0-20)

# New Vulnerabilities Tested in SecureScout

## • 18751 Mozilla Firefox - Re-use of freed object due to scope confusion Vulnerability (Remote File Checking)

A memory corruption flaw leading to code execution was reported by security researcher Nils of MWR InfoSecurity during the 2010 Pwn2Own contest sponsored by TippingPoint's Zero Day Initiative. By moving DOM nodes between documents Nils found a case where the moved node incorrectly retained its old scope. If garbage collection could be triggered at the right time then Firefox would later use this freed object.

The issue has been fixed in Firefox 3.6.3.

Only Firefox versions 3.6.x are affected.

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

### References:

\* MISC:

<http://dvlabs.tippingpoint.com/blog/2010/02/15/pwn2own-2010>

\* MISC:

[http://news.cnet.com/8301-27080\\_3-20001126-245.html](http://news.cnet.com/8301-27080_3-20001126-245.html)

\* MISC:

<http://twitter.com/thezdi/statuses/11005277222>

\* CONFIRM: mfsa2010-25

<http://www.mozilla.org/security/announce/2010/mfsa2010-25.html>

**CVE Reference:**

CVE-2010-1121 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18752 Mozilla Firefox - XmlDocument::load() doesn't check nsIContentPolicy Vulnerability (Remote File Checking)**

Mozilla community member Wladimir Palant reported that XML documents were failing to call certain security checks when loading new content. This could result in certain resources being loaded that would otherwise violate security policies set by the browser or installed add-ons.

The issue has been fixed in Firefox 3.5.9, and 3.6.2.

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

**References:**

\* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-24.html>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=490790](https://bugzilla.mozilla.org/show_bug.cgi?id=490790)

\* VUPEN: ADV-2010-0748

<http://www.vupen.com/english/advisories/2010/0748>

\* XF: firefox-xmldocumentload-weak-security(57396)

<http://xforce.iss.net/xforce/xfdb/57396>

**CVE Reference:**

CVE-2010-0182 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18753 Mozilla Thunderbird - XmlDocument::load() doesn't check nsIContentPolicy Vulnerability (Remote File Checking)**

Mozilla community member Wladimir Palant reported that XML documents were failing to call certain security checks when loading new content. This could result in certain resources being loaded that would otherwise violate security policies set by the browser or installed add-ons.

The issue has been fixed in Thunderbird 3.0.4.

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

**References:**

\* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-24.html>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=490790](https://bugzilla.mozilla.org/show_bug.cgi?id=490790)

\* VUPEN: ADV-2010-0748

<http://www.vupen.com/english/advisories/2010/0748>

\* XF: firefox-xmldocumentload-weak-security(57396)

<http://xforce.iss.net/xforce/xfdb/57396>

**CVE Reference:**

CVE-2010-0182 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18754 Mozilla Firefox - Image src redirect to mailto: URL opens email editor Vulnerability (Remote File Checking)**

phpBB developer Henry Sudhof reported that when an image tag points to a resource that redirects to a mailto: URL, the external mail handler application is launched. This issue poses no security threat to users but could create an annoyance when browsing a site that allows users to post arbitrary images.

The issue has been fixed in Firefox 3.5.9, and 3.6.2.

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

**References:**

\* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-23.html>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=452093](https://bugzilla.mozilla.org/show_bug.cgi?id=452093)

- \* SECUNIA: 39136  
<http://secunia.com/advisories/39136>
- \* VUPEN: ADV-2010-0748  
<http://www.vupen.com/english/advisories/2010/0748>
- \* XF: firefox-mailto-weak-security(57395)  
<http://xforce.iss.net/xforce/xfdb/57395>

#### CVE Reference:

CVE-2010-0181 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18755 Mozilla Firefox - Update NSS to support TLS renegotiation indication Vulnerability (Remote File Checking)

Mozilla developers added support in the Network Security Services module for preventing a type of man-in-the-middle attack against TLS using forced renegotiation.

The issue has been fixed in Firefox 3.5.9, and 3.6.2.

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

#### References:

- \* BUGTRAQ: 20091124 rPSA-2009-0155-1 httpd mod\_ssl  
<http://www.securityfocus.com/archive/1/archive/1/508075/100/0/threaded>
- \* BUGTRAQ: 20091118 TLS / SSLv3 vulnerability explained (DRAFT)  
<http://www.securityfocus.com/archive/1/archive/1/507952/100/0/threaded>
- \* BUGTRAQ: 20091130 TLS / SSLv3 vulnerability explained (New ways to leverage the vulnerability)  
<http://www.securityfocus.com/archive/1/archive/1/508130/100/0/threaded>
- \* FULLDISC: 20091111 Re: SSL/TLS MiTM PoC  
<http://seclists.org/fulldisclosure/2009/Nov/139>
- \* MLIST: [announce] 20091107 CVE-2009-3555 - apache/mod\_ssl vulnerability and mitigation  
<http://marc.info/?l=apache-httpd-announce&m=125755783724966&w=2>
- \* MLIST: [cryptography] 20091105 OpenSSL 0.9.8l released  
<http://marc.info/?l=cryptography&m=125752275331877&w=2>
- \* MLIST: [gnutls-devel] 20091105 Re: TLS renegotiation MITM  
<http://lists.gnu.org/archive/html/gnutls-devel/2009-11/msg00029.html>
- \* MLIST: [oss-security] 20091105 CVE-2009-3555 for TLS renegotiation MITM attacks  
<http://www.openwall.com/lists/oss-security/2009/11/05/3>
- \* MLIST: [oss-security] 20091105 Re: CVE-2009-3555 for TLS renegotiation MITM attacks  
<http://www.openwall.com/lists/oss-security/2009/11/05/5>
- \* MLIST: [oss-security] 20091107 Re: CVE-2009-3555 for TLS renegotiation MITM attacks  
<http://www.openwall.com/lists/oss-security/2009/11/06/3>
- \* MLIST: [oss-security] 20091107 Re: [TLS] CVE-2009-3555 for TLS renegotiation MITM attacks  
<http://www.openwall.com/lists/oss-security/2009/11/07/3>
- \* MLIST: [tls] 20091104 MITM attack on delayed TLS-client auth through renegotiation  
<http://www.ietf.org/mail-archive/web/tls/current/msg03928.html>
- \* MLIST: [tls] 20091104 TLS renegotiation issue  
<http://www.ietf.org/mail-archive/web/tls/current/msg03948.html>
- \* MLIST: [oss-security] 20091120 CVEs for nginx  
<http://www.openwall.com/lists/oss-security/2009/11/20/1>
- \* MLIST: [oss-security] 20091123 Re: CVEs for nginx  
<http://www.openwall.com/lists/oss-security/2009/11/23/10>
- \* MISC:  
<http://extendedsubset.com/?p=8>
- \* MISC:  
[http://extendedsubset.com/Renegotiating\\_TLS.pdf](http://extendedsubset.com/Renegotiating_TLS.pdf)
- \* MISC:  
<http://www.betanews.com/article/1257452450>
- \* MISC:  
[http://www.educatedguesswork.org/2009/11/understanding\\_the\\_tls\\_renegoti.html](http://www.educatedguesswork.org/2009/11/understanding_the_tls_renegoti.html)
- \* MISC:  
<http://www.links.org/?p=780>
- \* MISC:  
<http://www.tombom.co.uk/blog/?p=85>
- \* MISC:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=526689](https://bugzilla.mozilla.org/show_bug.cgi?id=526689)
- \* MISC:  
<https://svn.resiprocate.org/rep/ietf-drafts/ekr/draft-rescorla-tls-renegotiate.txt>
- \* MISC:  
<http://blogs.iss.net/archive/sslmitmiscsrf.html>

\* MISC:  
<http://www.links.org/?p=786>

\* MISC:  
<http://www.links.org/?p=789>

\* MISC:  
<http://www.securegoose.org/2009/11/tls-renegotiation-vulnerability-cve.html>

\* MISC:  
<http://blog.g-sec.lu/2009/11/tls-ssl3-renegotiation-vulnerability.html>

\* MISC:  
<http://clicky.me/tlsvuln>

\* MISC:  
<https://support.f5.com/kb/en-us/solutions/public/10000/700/sol10737.html>

\* CONFIRM:  
[http://blogs.sun.com/security/entry/vulnerability\\_in\\_tls\\_protocol\\_during](http://blogs.sun.com/security/entry/vulnerability_in_tls_protocol_during)

\* CONFIRM:  
<http://kbase.redhat.com/faq/docs/DOC-20491>

\* CONFIRM:  
[https://bugzilla.redhat.com/show\\_bug.cgi?id=533125](https://bugzilla.redhat.com/show_bug.cgi?id=533125)

\* CONFIRM:  
<http://support.citrix.com/article/CTX123359>

\* CONFIRM:  
<http://sysoev.ru/nginx/patch.cve-2009-3555.txt>

\* CONFIRM:  
<http://wiki.rpath.com/Advisories:rPSA-2009-0155>

\* CONFIRM:  
<http://www.ingate.com/Relnote.php?ver=481>

\* CONFIRM:  
<http://www-01.ibm.com/support/docview.wss?uid=swg24025312>

\* CONFIRM:  
[http://www.proftpd.org/docs/RELEASE\\_NOTES-1.3.2c](http://www.proftpd.org/docs/RELEASE_NOTES-1.3.2c)

\* CONFIRM:  
<http://support.apple.com/kb/HT4004>

\* CONFIRM:  
[http://support.zeus.com/zws/media/docs/4.3/RELEASE\\_NOTES](http://support.zeus.com/zws/media/docs/4.3/RELEASE_NOTES)

\* CONFIRM:  
[http://support.zeus.com/zws/news/2010/01/13/zws\\_4\\_3r5\\_released](http://support.zeus.com/zws/news/2010/01/13/zws_4_3r5_released)

\* CONFIRM:  
<http://www.arubanetworks.com/support/alerts/aid-020810.txt>

\* CONFIRM:  
<http://support.avaya.com/css/P8/documents/100070150>

\* CONFIRM:  
<http://www.mozilla.org/security/announce/2010/mfsa2010-22.html>

\* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=545755](https://bugzilla.mozilla.org/show_bug.cgi?id=545755)

\* AIXAPAR: PM00675  
<http://www-1.ibm.com/support/search.wss?rs=0&q=PM00675&apar=only>

\* APPLE: APPLE-SA-2010-01-19-1  
<http://lists.apple.com/archives/security-announce/2010/Jan/msg00000.html>

\* CISCO: 20091109 Transport Layer Security Renegotiation Vulnerability  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080b01d1d.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080b01d1d.shtml)

\* DEBIAN: DSA-1934  
<http://www.debian.org/security/2009/dsa-1934>

\* FEDORA: FEDORA-2009-12750  
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00428.html>

\* FEDORA: FEDORA-2009-12775  
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00442.html>

\* FEDORA: FEDORA-2009-12782  
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00449.html>

\* FEDORA: FEDORA-2009-12968  
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00634.html>

\* FEDORA: FEDORA-2009-12604  
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00645.html>

\* FEDORA: FEDORA-2009-12229  
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg01029.html>

\* FEDORA: FEDORA-2009-12305  
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg01020.html>

\* FEDORA: FEDORA-2009-12606  
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00944.html>

\* GENTOO: GLSA-200912-01

<http://security.gentoo.org/glsa/glsa-200912-01.xml>  
\* HP: HPSBUX02482  
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01945686>  
\* OPENBSD: [4.5] 010: SECURITY FIX: November 26, 2009  
[http://openbsd.org/errata45.html#010\\_openssl](http://openbsd.org/errata45.html#010_openssl)  
\* OPENBSD: [4.6] 004: SECURITY FIX: November 26, 2009  
[http://openbsd.org/errata46.html#004\\_openssl](http://openbsd.org/errata46.html#004_openssl)  
\* REDHAT: RHSA-2010:0119  
<http://www.redhat.com/support/errata/RHSA-2010-0119.html>  
\* REDHAT: RHSA-2010:0155  
<http://www.redhat.com/support/errata/RHSA-2010-0155.html>  
\* REDHAT: RHSA-2010:0167  
<http://www.redhat.com/support/errata/RHSA-2010-0167.html>  
\* SUNALERT: 273029  
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-273029-1>  
\* SUNALERT: 273350  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-273350-1>  
\* SUNALERT: 274990  
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-274990-1>  
\* SUSE: SUSE-SA:2009:057  
<http://lists.opensuse.org/opensuse-security-announce/2009-11/msg00009.html>  
\* CERT-VN: VU#120541  
<http://www.kb.cert.org/vuls/id/120541>  
\* BID: 36935  
<http://www.securityfocus.com/bid/36935>  
\* OSVDB: 60521  
<http://osvdb.org/60521>  
\* OSVDB: 60972  
<http://osvdb.org/60972>  
\* OSVDB: 62210  
<http://osvdb.org/62210>  
\* SECTRACK: 1023148  
<http://securitytracker.com/id?1023148>  
\* SECTRACK: 1023163  
<http://www.securitytracker.com/id?1023163>  
\* SECTRACK: 1023204  
<http://www.securitytracker.com/id?1023204>  
\* SECTRACK: 1023205  
<http://www.securitytracker.com/id?1023205>  
\* SECTRACK: 1023206  
<http://www.securitytracker.com/id?1023206>  
\* SECTRACK: 1023207  
<http://www.securitytracker.com/id?1023207>  
\* SECTRACK: 1023208  
<http://www.securitytracker.com/id?1023208>  
\* SECTRACK: 1023209  
<http://www.securitytracker.com/id?1023209>  
\* SECTRACK: 1023210  
<http://www.securitytracker.com/id?1023210>  
\* SECTRACK: 1023211  
<http://www.securitytracker.com/id?1023211>  
\* SECTRACK: 1023212  
<http://www.securitytracker.com/id?1023212>  
\* SECTRACK: 1023215  
<http://www.securitytracker.com/id?1023215>  
\* SECTRACK: 1023216  
<http://www.securitytracker.com/id?1023216>  
\* SECTRACK: 1023217  
<http://www.securitytracker.com/id?1023217>  
\* SECTRACK: 1023218  
<http://www.securitytracker.com/id?1023218>  
\* SECTRACK: 1023219  
<http://www.securitytracker.com/id?1023219>  
\* SECTRACK: 1023243  
<http://www.securitytracker.com/id?1023243>  
\* SECTRACK: 1023270  
<http://www.securitytracker.com/id?1023270>  
\* SECTRACK: 1023271  
<http://www.securitytracker.com/id?1023271>

\* SECTRACK: 1023272  
<http://www.securitytracker.com/id?1023272>  
\* SECTRACK: 1023273  
<http://www.securitytracker.com/id?1023273>  
\* SECTRACK: 1023274  
<http://www.securitytracker.com/id?1023274>  
\* SECTRACK: 1023275  
<http://www.securitytracker.com/id?1023275>  
\* SECTRACK: 1023411  
<http://www.securitytracker.com/id?1023411>  
\* SECTRACK: 1023426  
<http://www.securitytracker.com/id?1023426>  
\* SECTRACK: 1023427  
<http://www.securitytracker.com/id?1023427>  
\* SECTRACK: 1023428  
<http://www.securitytracker.com/id?1023428>  
\* SECUNIA: 37291  
<http://secunia.com/advisories/37291>  
\* SECUNIA: 37292  
<http://secunia.com/advisories/37292>  
\* SECUNIA: 37320  
<http://secunia.com/advisories/37320>  
\* SECUNIA: 37501  
<http://secunia.com/advisories/37501>  
\* SECUNIA: 37504  
<http://secunia.com/advisories/37504>  
\* SECUNIA: 37656  
<http://secunia.com/advisories/37656>  
\* SECUNIA: 37675  
<http://secunia.com/advisories/37675>  
\* SECUNIA: 37604  
<http://secunia.com/advisories/37604>  
\* SECUNIA: 37640  
<http://secunia.com/advisories/37640>  
\* SECUNIA: 37859  
<http://secunia.com/advisories/37859>  
\* SECUNIA: 38056  
<http://secunia.com/advisories/38056>  
\* SECUNIA: 38241  
<http://secunia.com/advisories/38241>  
\* SECUNIA: 38484  
<http://secunia.com/advisories/38484>  
\* SECUNIA: 38003  
<http://secunia.com/advisories/38003>  
\* SECUNIA: 38020  
<http://secunia.com/advisories/38020>  
\* SECUNIA: 38687  
<http://secunia.com/advisories/38687>  
\* SECUNIA: 39136  
<http://secunia.com/advisories/39136>  
\* SECUNIA: 39242  
<http://secunia.com/advisories/39242>  
\* SECUNIA: 39243  
<http://secunia.com/advisories/39243>  
\* VUPEN: ADV-2009-3164  
<http://www.vupen.com/english/advisories/2009/3164>  
\* VUPEN: ADV-2009-3165  
<http://www.vupen.com/english/advisories/2009/3165>  
\* VUPEN: ADV-2009-3205  
<http://www.vupen.com/english/advisories/2009/3205>  
\* VUPEN: ADV-2009-3220  
<http://www.vupen.com/english/advisories/2009/3220>  
\* VUPEN: ADV-2009-3353  
<http://www.vupen.com/english/advisories/2009/3353>  
\* VUPEN: ADV-2009-3354  
<http://www.vupen.com/english/advisories/2009/3354>  
\* VUPEN: ADV-2009-3484  
<http://www.vupen.com/english/advisories/2009/3484>  
\* VUPEN: ADV-2009-3521

<http://www.vupen.com/english/advisories/2009/3521>

\* VUPEN: ADV-2009-3587

<http://www.vupen.com/english/advisories/2009/3587>

\* VUPEN: ADV-2010-0173

<http://www.vupen.com/english/advisories/2010/0173>

\* VUPEN: ADV-2010-0086

<http://www.vupen.com/english/advisories/2010/0086>

\* VUPEN: ADV-2010-0748

<http://www.vupen.com/english/advisories/2010/0748>

\* XF: tls-renegotiation-weak-security(54158)

<http://xforce.iss.net/xforce/xfdb/54158>

#### CVE Reference:

CVE-2009-3555 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18756 Mozilla Thunderbird - Update NSS to support TLS renegotiation indication Vulnerability (Remote File Checking)

Mozilla developers added support in the Network Security Services module for preventing a type of man-in-the-middle attack against TLS using forced renegotiation.

The issue has been fixed in Thunderbird 3.0.4.

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

#### References:

\* BUGTRAQ: 20091124 rPSA-2009-0155-1 httpd mod\_ssl

<http://www.securityfocus.com/archive/1/archive/1/508075/100/0/threaded>

\* BUGTRAQ: 20091118 TLS / SSLv3 vulnerability explained (DRAFT)

<http://www.securityfocus.com/archive/1/archive/1/507952/100/0/threaded>

\* BUGTRAQ: 20091130 TLS / SSLv3 vulnerability explained (New ways to leverage the vulnerability)

<http://www.securityfocus.com/archive/1/archive/1/508130/100/0/threaded>

\* FULLDISC: 20091111 Re: SSL/TLS MiTM PoC

<http://seclists.org/fulldisclosure/2009/Nov/139>

\* MLIST: [announce] 20091107 CVE-2009-3555 - apache/mod\_ssl vulnerability and mitigation

<http://marc.info/?l=apache-httpd-announce&m=125755783724966&w=2>

\* MLIST: [cryptography] 20091105 OpenSSL 0.9.8l released

<http://marc.info/?l=cryptography&m=125752275331877&w=2>

\* MLIST: [gnutls-devel] 20091105 Re: TLS renegotiation MITM

<http://lists.gnu.org/archive/html/gnutls-devel/2009-11/msg00029.html>

\* MLIST: [oss-security] 20091105 CVE-2009-3555 for TLS renegotiation MITM attacks

<http://www.openwall.com/lists/oss-security/2009/11/05/3>

\* MLIST: [oss-security] 20091105 Re: CVE-2009-3555 for TLS renegotiation MITM attacks

<http://www.openwall.com/lists/oss-security/2009/11/05/5>

\* MLIST: [oss-security] 20091107 Re: CVE-2009-3555 for TLS renegotiation MITM attacks

<http://www.openwall.com/lists/oss-security/2009/11/06/3>

\* MLIST: [oss-security] 20091107 Re: [TLS] CVE-2009-3555 for TLS renegotiation MITM attacks

<http://www.openwall.com/lists/oss-security/2009/11/07/3>

\* MLIST: [tls] 20091104 MITM attack on delayed TLS-client auth through renegotiation

<http://www.ietf.org/mail-archive/web/tls/current/msg03928.html>

\* MLIST: [tls] 20091104 TLS renegotiation issue

<http://www.ietf.org/mail-archive/web/tls/current/msg03948.html>

\* MLIST: [oss-security] 20091120 CVEs for nginx

<http://www.openwall.com/lists/oss-security/2009/11/20/1>

\* MLIST: [oss-security] 20091123 Re: CVEs for nginx

<http://www.openwall.com/lists/oss-security/2009/11/23/10>

\* MISC:

<http://extendedsubset.com/?p=8>

\* MISC:

[http://extendedsubset.com/Renegotiating\\_TLS.pdf](http://extendedsubset.com/Renegotiating_TLS.pdf)

\* MISC:

<http://www.betanews.com/article/1257452450>

\* MISC:

[http://www.educatedguesswork.org/2009/11/understanding\\_the\\_tls\\_renegoti.html](http://www.educatedguesswork.org/2009/11/understanding_the_tls_renegoti.html)

\* MISC:

<http://www.links.org/?p=780>

\* MISC:

<http://www.tombom.co.uk/blog/?p=85>

\* MISC:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=526689](https://bugzilla.mozilla.org/show_bug.cgi?id=526689)  
\* MISC:  
<https://svn.resiprocate.org/rep/ietf-drafts/ekr/draft-rescorla-tls-renegotiate.txt>  
\* MISC:  
<http://blogs.iss.net/archive/sslmitmiscsrf.html>  
\* MISC:  
<http://www.links.org/?p=786>  
\* MISC:  
<http://www.links.org/?p=789>  
\* MISC:  
<http://www.securegoose.org/2009/11/tls-renegotiation-vulnerability-cve.html>  
\* MISC:  
<http://blog.g-sec.lu/2009/11/tls-ssl3-renegotiation-vulnerability.html>  
\* MISC:  
<http://clicky.me/tlsvuln>  
\* MISC:  
<https://support.f5.com/kb/en-us/solutions/public/10000/700/sol10737.html>  
\* CONFIRM:  
[http://blogs.sun.com/security/entry/vulnerability\\_in\\_tls\\_protocol\\_during](http://blogs.sun.com/security/entry/vulnerability_in_tls_protocol_during)  
\* CONFIRM:  
<http://kbase.redhat.com/faq/docs/DOC-20491>  
\* CONFIRM:  
[https://bugzilla.redhat.com/show\\_bug.cgi?id=533125](https://bugzilla.redhat.com/show_bug.cgi?id=533125)  
\* CONFIRM:  
<http://support.citrix.com/article/CTX123359>  
\* CONFIRM:  
<http://sysoev.ru/nginx/patch.cve-2009-3555.txt>  
\* CONFIRM:  
<http://wiki.rpath.com/Advisories:rPSA-2009-0155>  
\* CONFIRM:  
<http://www.ingate.com/Relnote.php?ver=481>  
\* CONFIRM:  
<http://www-01.ibm.com/support/docview.wss?uid=swg24025312>  
\* CONFIRM:  
[http://www.proftpd.org/docs/RELEASE\\_NOTES-1.3.2c](http://www.proftpd.org/docs/RELEASE_NOTES-1.3.2c)  
\* CONFIRM:  
<http://support.apple.com/kb/HT4004>  
\* CONFIRM:  
[http://support.zeus.com/zws/media/docs/4.3/RELEASE\\_NOTES](http://support.zeus.com/zws/media/docs/4.3/RELEASE_NOTES)  
\* CONFIRM:  
[http://support.zeus.com/zws/news/2010/01/13/zws\\_4\\_3r5\\_released](http://support.zeus.com/zws/news/2010/01/13/zws_4_3r5_released)  
\* CONFIRM:  
<http://www.arubanetworks.com/support/alerts/aid-020810.txt>  
\* CONFIRM:  
<http://support.avaya.com/css/P8/documents/100070150>  
\* CONFIRM:  
<http://www.mozilla.org/security/announce/2010/mfsa2010-22.html>  
\* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=545755](https://bugzilla.mozilla.org/show_bug.cgi?id=545755)  
\* AIXAPAR: PM00675  
<http://www-1.ibm.com/support/search.wss?rs=0&g=PM00675&apar=only>  
\* APPLE: APPLE-SA-2010-01-19-1  
<http://lists.apple.com/archives/security-announce/2010/Jan/msg00000.html>  
\* CISCO: 20091109 Transport Layer Security Renegotiation Vulnerability  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080b01d1d.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080b01d1d.shtml)  
\* DEBIAN: DSA-1934  
<http://www.debian.org/security/2009/dsa-1934>  
\* FEDORA: FEDORA-2009-12750  
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00428.html>  
\* FEDORA: FEDORA-2009-12775  
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00442.html>  
\* FEDORA: FEDORA-2009-12782  
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00449.html>  
\* FEDORA: FEDORA-2009-12968  
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00634.html>  
\* FEDORA: FEDORA-2009-12604  
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00645.html>  
\* FEDORA: FEDORA-2009-12229  
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg01029.html>

\* FEDORA: FEDORA-2009-12305  
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg01020.html>

\* FEDORA: FEDORA-2009-12606  
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00944.html>

\* GENTOO: GLSA-200912-01  
<http://security.gentoo.org/glsa/glsa-200912-01.xml>

\* HP: HPSBUX02482  
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01945686>

\* OPENBSD: [4.5] 010: SECURITY FIX: November 26, 2009  
[http://openbsd.org/errata45.html#010\\_openssl](http://openbsd.org/errata45.html#010_openssl)

\* OPENBSD: [4.6] 004: SECURITY FIX: November 26, 2009  
[http://openbsd.org/errata46.html#004\\_openssl](http://openbsd.org/errata46.html#004_openssl)

\* REDHAT: RHSA-2010:0119  
<http://www.redhat.com/support/errata/RHSA-2010-0119.html>

\* REDHAT: RHSA-2010:0155  
<http://www.redhat.com/support/errata/RHSA-2010-0155.html>

\* REDHAT: RHSA-2010:0167  
<http://www.redhat.com/support/errata/RHSA-2010-0167.html>

\* SUNALERT: 273029  
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-273029-1>

\* SUNALERT: 273350  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-273350-1>

\* SUNALERT: 274990  
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-274990-1>

\* SUSE: SUSE-SA:2009:057  
<http://lists.opensuse.org/opensuse-security-announce/2009-11/msg00009.html>

\* CERT-VN: VU#120541  
<http://www.kb.cert.org/vuls/id/120541>

\* BID: 36935  
<http://www.securityfocus.com/bid/36935>

\* OSVDB: 60521  
<http://osvdb.org/60521>

\* OSVDB: 60972  
<http://osvdb.org/60972>

\* OSVDB: 62210  
<http://osvdb.org/62210>

\* SECTRACK: 1023148  
<http://securitytracker.com/id?1023148>

\* SECTRACK: 1023163  
<http://www.securitytracker.com/id?1023163>

\* SECTRACK: 1023204  
<http://www.securitytracker.com/id?1023204>

\* SECTRACK: 1023205  
<http://www.securitytracker.com/id?1023205>

\* SECTRACK: 1023206  
<http://www.securitytracker.com/id?1023206>

\* SECTRACK: 1023207  
<http://www.securitytracker.com/id?1023207>

\* SECTRACK: 1023208  
<http://www.securitytracker.com/id?1023208>

\* SECTRACK: 1023209  
<http://www.securitytracker.com/id?1023209>

\* SECTRACK: 1023210  
<http://www.securitytracker.com/id?1023210>

\* SECTRACK: 1023211  
<http://www.securitytracker.com/id?1023211>

\* SECTRACK: 1023212  
<http://www.securitytracker.com/id?1023212>

\* SECTRACK: 1023215  
<http://www.securitytracker.com/id?1023215>

\* SECTRACK: 1023216  
<http://www.securitytracker.com/id?1023216>

\* SECTRACK: 1023217  
<http://www.securitytracker.com/id?1023217>

\* SECTRACK: 1023218  
<http://www.securitytracker.com/id?1023218>

\* SECTRACK: 1023219  
<http://www.securitytracker.com/id?1023219>

\* SECTRACK: 1023243

<http://www.securitytracker.com/id?1023243>  
\* SECTRACK: 1023270  
<http://www.securitytracker.com/id?1023270>  
\* SECTRACK: 1023271  
<http://www.securitytracker.com/id?1023271>  
\* SECTRACK: 1023272  
<http://www.securitytracker.com/id?1023272>  
\* SECTRACK: 1023273  
<http://www.securitytracker.com/id?1023273>  
\* SECTRACK: 1023274  
<http://www.securitytracker.com/id?1023274>  
\* SECTRACK: 1023275  
<http://www.securitytracker.com/id?1023275>  
\* SECTRACK: 1023411  
<http://www.securitytracker.com/id?1023411>  
\* SECTRACK: 1023426  
<http://www.securitytracker.com/id?1023426>  
\* SECTRACK: 1023427  
<http://www.securitytracker.com/id?1023427>  
\* SECTRACK: 1023428  
<http://www.securitytracker.com/id?1023428>  
\* SECUNIA: 37291  
<http://secunia.com/advisories/37291>  
\* SECUNIA: 37292  
<http://secunia.com/advisories/37292>  
\* SECUNIA: 37320  
<http://secunia.com/advisories/37320>  
\* SECUNIA: 37501  
<http://secunia.com/advisories/37501>  
\* SECUNIA: 37504  
<http://secunia.com/advisories/37504>  
\* SECUNIA: 37656  
<http://secunia.com/advisories/37656>  
\* SECUNIA: 37675  
<http://secunia.com/advisories/37675>  
\* SECUNIA: 37604  
<http://secunia.com/advisories/37604>  
\* SECUNIA: 37640  
<http://secunia.com/advisories/37640>  
\* SECUNIA: 37859  
<http://secunia.com/advisories/37859>  
\* SECUNIA: 38056  
<http://secunia.com/advisories/38056>  
\* SECUNIA: 38241  
<http://secunia.com/advisories/38241>  
\* SECUNIA: 38484  
<http://secunia.com/advisories/38484>  
\* SECUNIA: 38003  
<http://secunia.com/advisories/38003>  
\* SECUNIA: 38020  
<http://secunia.com/advisories/38020>  
\* SECUNIA: 38687  
<http://secunia.com/advisories/38687>  
\* SECUNIA: 39136  
<http://secunia.com/advisories/39136>  
\* SECUNIA: 39242  
<http://secunia.com/advisories/39242>  
\* SECUNIA: 39243  
<http://secunia.com/advisories/39243>  
\* VUPEN: ADV-2009-3164  
<http://www.vupen.com/english/advisories/2009/3164>  
\* VUPEN: ADV-2009-3165  
<http://www.vupen.com/english/advisories/2009/3165>  
\* VUPEN: ADV-2009-3205  
<http://www.vupen.com/english/advisories/2009/3205>  
\* VUPEN: ADV-2009-3220  
<http://www.vupen.com/english/advisories/2009/3220>  
\* VUPEN: ADV-2009-3353  
<http://www.vupen.com/english/advisories/2009/3353>

- \* VUPEN: ADV-2009-3354  
<http://www.vupen.com/english/advisories/2009/3354>
- \* VUPEN: ADV-2009-3484  
<http://www.vupen.com/english/advisories/2009/3484>
- \* VUPEN: ADV-2009-3521  
<http://www.vupen.com/english/advisories/2009/3521>
- \* VUPEN: ADV-2009-3587  
<http://www.vupen.com/english/advisories/2009/3587>
- \* VUPEN: ADV-2010-0173  
<http://www.vupen.com/english/advisories/2010/0173>
- \* VUPEN: ADV-2010-0086  
<http://www.vupen.com/english/advisories/2010/0086>
- \* VUPEN: ADV-2010-0748  
<http://www.vupen.com/english/advisories/2010/0748>
- \* XF: tls-renegotiation-weak-security(54158)  
<http://xforce.iss.net/xforce/xfdb/54158>

#### CVE Reference:

CVE-2009-3555 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18757 Mozilla Firefox - Arbitrary code execution with Firebug XMLHttpRequestSpy Vulnerability (Remote File Checking)

Mozilla security researcher moz\_bug\_r\_a4 reported that the XMLHttpRequestSpy module in the Firebug add-on was exposing an underlying chrome privilege escalation vulnerability. When the XMLHttpRequestSpy object was created, it would attach various properties of itself to objects defined in web content, which were not being properly wrapped to prevent their exposure to chrome privileged objects. This could result in an attacker running arbitrary JavaScript on a victim's machine, though it required the victim to have Firebug installed, so the overall severity of the issue was determined to be High.

The issue has been fixed in Firefox 3.0.19, and 3.5.8.

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

#### References:

- \* CONFIRM:  
<http://www.mozilla.org/security/announce/2010/mfsa2010-21.html>
- \* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=504021](https://bugzilla.mozilla.org/show_bug.cgi?id=504021)
- \* REDHAT: RHSA-2010:0332  
<http://www.redhat.com/support/errata/RHSA-2010-0332.html>
- \* SECTRACK: 1023783  
<http://securitytracker.com/id?1023783>
- \* SECUNIA: 3924  
<http://secunia.com/advisories/3924>
- \* SECUNIA: 39243  
<http://secunia.com/advisories/39243>
- \* VUPEN: ADV-2010-0748  
<http://www.vupen.com/english/advisories/2010/0748>
- \* VUPEN: ADV-2010-0764  
<http://www.vupen.com/english/advisories/2010/0764>
- \* XF: firefox-firebug-code-execution(57394)  
<http://xforce.iss.net/xforce/xfdb/57394>

#### CVE Reference:

CVE-2010-0179 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18758 Mozilla Firefox - Chrome privilege escalation via forced URL drag and drop Vulnerability (Remote File Checking)

Security researcher Paul Stone reported that a browser applet could be used to turn a simple mouse click into a drag-and-drop action, potentially resulting in the unintended loading of resources in a user's browser. This behavior could be used twice in succession to first load a privileged chrome: URL in a victim's browser, then load a malicious javascript: URL on top of the same document resulting in arbitrary script execution with chrome privileges.

The issue has been fixed in Firefox 3.0.19, 3.5.9, and 3.6.2.

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

#### References:

\* CONFIRM:  
<http://www.mozilla.org/security/announce/2010/mfsa2010-20.html>  
\* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=546909](https://bugzilla.mozilla.org/show_bug.cgi?id=546909)  
\* REDHAT: RHSA-2010:0332  
<http://www.redhat.com/support/errata/RHSA-2010-0332.html>  
\* SECTRACK: 1023776  
<http://securitytracker.com/id?1023776>  
\* SECUNIA: 39136  
<http://secunia.com/advisories/39136>  
\* SECUNIA: 39240  
<http://secunia.com/advisories/39240>  
\* SECUNIA: 39243  
<http://secunia.com/advisories/39243>  
\* VUPEN: ADV-2010-0748  
<http://www.vupen.com/english/advisories/2010/0748>  
\* VUPEN: ADV-2010-0764  
<http://www.vupen.com/english/advisories/2010/0764>  
\* XF: firefox-draganddrop-code-execution(57391)  
<http://xforce.iss.net/xforce/xfdb/57391>

#### CVE Reference:

CVE-2010-0178 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### ● 18759 Mozilla Firefox - Dangling pointer vulnerability in nsPluginArray Vulnerability (Remote File Checking)

Security researcher regenrecht reported via TippingPoint's Zero Day Initiative an error in the implementation of the window.navigator.plugins object. When a page reloads, the plugins array would reallocate all of its members without checking for existing references to each member. This could result in the deletion of objects for which valid pointers still exist. An attacker could use this vulnerability to crash a victim's browser and run arbitrary code on the victim's machine.

The issue has been fixed in Firefox 3.0.19, 3.5.9, and 3.6.2.

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

#### References:

\* CONFIRM:  
<http://www.mozilla.org/security/announce/2010/mfsa2010-19.html>  
\* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=538310](https://bugzilla.mozilla.org/show_bug.cgi?id=538310)  
\* REDHAT: RHSA-2010:0332  
<http://www.redhat.com/support/errata/RHSA-2010-0332.html>  
\* REDHAT: RHSA-2010:0333  
<http://www.redhat.com/support/errata/RHSA-2010-0333.html>  
\* SECTRACK: 1023776  
<http://securitytracker.com/id?1023776>  
\* SECUNIA: 38566  
<http://secunia.com/advisories/38566>  
\* SECUNIA: 39117  
<http://secunia.com/advisories/39117>  
\* SECUNIA: 39136  
<http://secunia.com/advisories/39136>  
\* SECUNIA: 39240  
<http://secunia.com/advisories/39240>  
\* SECUNIA: 39243  
<http://secunia.com/advisories/39243>  
\* VUPEN: ADV-2010-0748  
<http://www.vupen.com/english/advisories/2010/0748>  
\* VUPEN: ADV-2010-0764  
<http://www.vupen.com/english/advisories/2010/0764>  
\* VUPEN: ADV-2010-0765  
<http://www.vupen.com/english/advisories/2010/0765>  
\* XF: firefox-nspluginarray-code-execution(57393)  
<http://xforce.iss.net/xforce/xfdb/57393>

#### CVE Reference:

CVE-2010-0177 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## • 18760 Mozilla Firefox - Dangling pointer vulnerability in nsTreeContentView Vulnerability (Remote File Checking)

Security researcher regenrecht reported via TippingPoint's Zero Day Initiative an error in the way <option> elements are inserted into a XUL tree <optgroup>. In certain cases, the number of references to an <option> element is under-counted so that when the element is deleted, a live pointer to its old location is kept around and may later be used. An attacker could potentially use these conditions to run arbitrary code on a victim's computer.

The issue has been fixed in Firefox 3.0.19, 3.5.9, and 3.6.2.

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

### References:

\* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-18.html>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=538308](https://bugzilla.mozilla.org/show_bug.cgi?id=538308)

\* FEDORA: FEDORA-2010-5526

<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038367.html>

\* FEDORA: FEDORA-2010-5539

<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038378.html>

\* REDHAT: RHSA-2010:0332

<http://www.redhat.com/support/errata/RHSA-2010-0332.html>

\* REDHAT: RHSA-2010:0333

<http://www.redhat.com/support/errata/RHSA-2010-0333.html>

\* SECTrack: 1023776

<http://securitytracker.com/id?1023776>

\* SECTrack: 1023782

<http://securitytracker.com/id?1023782>

\* SECUNIA: 38566

<http://secunia.com/advisories/38566>

\* SECUNIA: 39117

<http://secunia.com/advisories/39117>

\* SECUNIA: 39136

<http://secunia.com/advisories/39136>

\* SECUNIA: 39204

<http://secunia.com/advisories/39204>

\* SECUNIA: 39240

<http://secunia.com/advisories/39240>

\* SECUNIA: 39242

<http://secunia.com/advisories/39242>

\* SECUNIA: 39243

<http://secunia.com/advisories/39243>

\* VUPEN: ADV-2010-0748

<http://www.vupen.com/english/advisories/2010/0748>

\* VUPEN: ADV-2010-0764

<http://www.vupen.com/english/advisories/2010/0764>

\* VUPEN: ADV-2010-0765

<http://www.vupen.com/english/advisories/2010/0765>

\* XF: firefox-nsTreeContentView-code-exec(57392)

<http://xforce.iss.net/xforce/xfdb/57392>

### CVE Reference:

CVE-2010-0176 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

### • CVE-2010-0009 Apache CVSS 2.0 Score = 7.5

Apache CouchDB 0.8.0 through 0.10.1 allows remote attackers to obtain sensitive information by measuring the completion time of operations that verify (1) hashes or (2) passwords.

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

### References:

CONFIRM: <http://couchdb.apache.org/security.html>

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=578572](https://bugzilla.redhat.com/show_bug.cgi?id=578572)

BID: <http://www.securityfocus.com/bid/39116>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/510427/100/0/threaded>

OSVDB: <http://www.osvdb.org/63350>

SECUNIA: <http://secunia.com/advisories/39146>

BUGTRAQ: <http://archives.neohapsis.com/archives/bugtraq/2010-03/0267.html>

**CVE Reference:** [CVE-2010-0009](#)

• **CVE-2010-1244 Apache CVSS 2.0 Score = 6.8**

Cross-site request forgery (CSRF) vulnerability in createDestination.action in Apache ActiveMQ before 5.3.1 allows remote attackers to hijack the authentication of unspecified victims for requests that create queues via the JMSDestination parameter in a queue action.

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

**References:**

CONFIRM: <http://activemq.apache.org/activemq-531-release.html>

CONFIRM: <https://issues.apache.org/activemq/browse/AMQ-2625>

CONFIRM: <https://issues.apache.org/activemq/browse/AMQ-2613>

XF: <http://xforce.iss.net/xforce/xfdb/57398>

SECUNIA: <http://secunia.com/advisories/39223>

**CVE Reference:** [CVE-2010-1244](#)

• **CVE-2010-0684 Apache CVSS 2.0 Score = 3.5**

Cross-site scripting (XSS) vulnerability in createDestination.action in Apache ActiveMQ before 5.3.1 allows remote authenticated users to inject arbitrary web script or HTML via the JMSDestination parameter in a queue action.

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

**References:**

BID: <http://www.securityfocus.com/bid/39119>

CONFIRM: <http://activemq.apache.org/activemq-531-release.html>

CONFIRM: <https://issues.apache.org/activemq/browse/AMQ-2625>

CONFIRM: <https://issues.apache.org/activemq/browse/AMQ-2613>

XF: <http://xforce.iss.net/xforce/xfdb/57397>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/510419/100/0/threaded>

MISC: <http://www.rajatswarup.com/CVE-2010-0684.txt>

SECTRACK: <http://securitytracker.com/id?1023778>

SECUNIA: <http://secunia.com/advisories/39223>

**CVE Reference:** [CVE-2010-0684](#)

• **CVE-2010-1243 IBM CVSS 2.0 Score = 7.5**

The IBM Web Interface for Content Management (aka WEBi) before 1.0.4 creates persistent cookies on client workstations, which has unspecified impact and attack vectors.

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

**References:**

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg24025662>

VUPEN: <http://www.vupen.com/english/advisories/2010/0733>

SECUNIA: <http://secunia.com/advisories/39186>

**CVE Reference:** [CVE-2010-1243](#)

• **CVE-2010-0174 Mozilla CVSS 2.0 Score = 10.0**

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.0.19, 3.5.x before 3.5.9, and 3.6.x before 3.6.2; Thunderbird before 3.0.4; and SeaMonkey before 2.0.4 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: Vulnerability Impact: Risk: **High**

**References:**

CONFIRM: [https://bugzilla.mozilla.org/show\\_bug.cgi?id=546530](https://bugzilla.mozilla.org/show_bug.cgi?id=546530)

CONFIRM: [https://bugzilla.mozilla.org/show\\_bug.cgi?id=499844](https://bugzilla.mozilla.org/show_bug.cgi?id=499844)

XF: <http://xforce.iss.net/xforce/xfdb/57389>

VUPEN: <http://www.vupen.com/english/advisories/2010/0765>

VUPEN: <http://www.vupen.com/english/advisories/2010/0764>

VUPEN: <http://www.vupen.com/english/advisories/2010/0748>

REDHAT: <http://www.redhat.com/support/errata/RHSA-2010-0333.html>

REDHAT: <http://www.redhat.com/support/errata/RHSA-2010-0332.html>

CONFIRM: <http://www.mozilla.org/security/announce/2010/mfsa2010-16.html>

SECTRACK: <http://securitytracker.com/id?1023781>

SECTRACK: <http://securitytracker.com/id?1023775>

SECUNIA: <http://secunia.com/advisories/39243>

SECUNIA: <http://secunia.com/advisories/39242>

SECUNIA: <http://secunia.com/advisories/39240>

SECUNIA: <http://secunia.com/advisories/39204>

SECUNIA: <http://secunia.com/advisories/39136>

SECUNIA: <http://secunia.com/advisories/39117>

SECUNIA: <http://secunia.com/advisories/38566>

FEDORA: <http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038378.html>

FEDORA: <http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038367.html>

**CVE Reference:** [CVE-2010-0174](#)

• **CVE-2003-1595 Novell CVSS 2.0 Score = 10.0**

NWFTPD.nlm before 5.04.05 in the FTP server in Novell NetWare 6.5 does not properly perform "intruder detection," which has unspecified impact and attack vectors.

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

**References:**

CONFIRM: <http://www.novell.com/support/viewContent.do?externalId=3238588&sliceId=1>

**CVE Reference:** [CVE-2003-1595](#)

• **CVE-2010-0176 Mozilla CVSS 2.0 Score = 9.3**

Mozilla Firefox before 3.0.19, 3.5.x before 3.5.9, and 3.6.x before 3.6.2; Thunderbird before 3.0.4; and SeaMonkey before 2.0.4 do not properly manage reference counts for option elements in a XUL tree optgroup, which might allow remote attackers to execute arbitrary code via unspecified vectors that trigger access to deleted elements, related to a "dangling pointer vulnerability."

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

**References:**

CONFIRM: [https://bugzilla.mozilla.org/show\\_bug.cgi?id=538308](https://bugzilla.mozilla.org/show_bug.cgi?id=538308)

XF: <http://xforce.iss.net/xforce/xfdb/57392>

VUPEN: <http://www.vupen.com/english/advisories/2010/0765>

VUPEN: <http://www.vupen.com/english/advisories/2010/0764>

VUPEN: <http://www.vupen.com/english/advisories/2010/0748>

REDHAT: <http://www.redhat.com/support/errata/RHSA-2010-0333.html>

REDHAT: <http://www.redhat.com/support/errata/RHSA-2010-0332.html>

CONFIRM: <http://www.mozilla.org/security/announce/2010/mfsa2010-18.html>

SECTRACK: <http://securitytracker.com/id?1023782>

SECTRACK: <http://securitytracker.com/id?1023776>

SECUNIA: <http://secunia.com/advisories/39243>

SECUNIA: <http://secunia.com/advisories/39242>

SECUNIA: <http://secunia.com/advisories/39240>

SECUNIA: <http://secunia.com/advisories/39204>

SECUNIA: <http://secunia.com/advisories/39136>

SECUNIA: <http://secunia.com/advisories/39117>

SECUNIA: <http://secunia.com/advisories/38566>

FEDORA: <http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038378.html>

FEDORA: <http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038367.html>

**CVE Reference:** [CVE-2010-0176](#)

• **CVE-2010-0179 Mozilla CVSS 2.0 Score = 9.3**

Mozilla Firefox before 3.0.19 and 3.5.x before 3.5.8, and SeaMonkey before 2.0.3, when the XMLHttpRequestSpy module in the Firebug add-on is used, does not properly handle interaction between the XMLHttpRequestSpy object and chrome privileged objects, which allows remote attackers to execute arbitrary JavaScript via a crafted HTTP response.

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

**References:**

CONFIRM: [https://bugzilla.mozilla.org/show\\_bug.cgi?id=504021](https://bugzilla.mozilla.org/show_bug.cgi?id=504021)

XF: <http://xforce.iss.net/xforce/xfdb/57394>

VUPEN: <http://www.vupen.com/english/advisories/2010/0764>

VUPEN: <http://www.vupen.com/english/advisories/2010/0748>

REDHAT: <http://www.redhat.com/support/errata/RHSA-2010-0332.html>

CONFIRM: <http://www.mozilla.org/security/announce/2010/mfsa2010-21.html>

SECTRAK: <http://securitytracker.com/id?1023783>

SECUNIA: <http://secunia.com/advisories/39243>

SECUNIA: <http://secunia.com/advisories/3924>

**CVE Reference:** [CVE-2010-0179](#)

### **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)