

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

Group working on patient data security standard. Some words on network baselining. We all love it, but.... Gartner report on data breeches.

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

• Group unveils first-of-its-kind standard to secure patient data

A health care industry coalition on Monday released a prescriptive security framework that organizations can use to safeguard patient records as they increasingly move online.

The framework, released by the Health Information Trust Alliance (HITRUST) -- which represents health care providers, pharmacies, insurers, biotech firms and medical device manufacturers -- is based on well-known standards such as COBIT, NIST and ISO 270001.

But this is the first benchmark developed specifically for protecting health data.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Group-unveils-first-of-its-kind-standard-to-secure-patient-data/article/128168/>

• Getting network baselining right

March 3, 2009 (Network World) While simple in concept, network baselining is often misunderstood.

The technique provides the network administrator insight into expected behavior on the network and subsequently, the ability to notice changes. People often think of expected behavior as always being good traffic, meaning that expected behavior of a network reflects when everything is running perfectly. This is incorrect. Think of expected behavior as known vs. unknown traffic.

But the reality is less than 5% of administrators make a practice of baselining, for reasons such as "we don't have the time to do baselines" or "things change too much to do baselines" or "I'm not going to hire a person or multiple people to keep baselines organized." In these tough economic times, such concerns need to be exposed for what they are: misconceptions.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9128915&source=rss_topic1

• **Legislator moves to limit Google Maps because of terrorist threat**

March 4, 2009 (Computerworld) A California state legislator has submitted a bill that would limit the amount of detail allowed in images available from applications such as Google Maps and Google Earth, contending that terrorists are using such online tools to plot attacks.

Anderson told Computerworld that he is looking to limit the amount of detail that Internet users can see.

Elaine Filadelfo, a spokeswoman for Google, said they are hoping to have a sit down with Anderson and talk about his concerns.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9128978&source=rss_topic1

• **Gartner: Data breaches hit 7.5 percent of all U.S. adults**

Financial fraud last year caused 7.5 percent of all adults in the United States to lose money, largely because of data breaches.

"Fraud victims are also more cautious about which brick-and-mortar stores they shop at and how they pay for goods when they get there, demonstrating more awareness of the risk of data breaches," said Avivah Litan, vice president and distinguished analyst at Gartner, in a news release.

Gartner found that financial losses were highest with new-account, credit card and brokerage fraud, with average losses per incident totaling \$1,097, \$929 and \$900, respectively. However, victims of brokerage, credit card and debit/ATM card fraud find it easiest to recover their losses, receiving an average of 100 percent, 86 percent, and 77 percent of the funds stolen, respectively.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Gartner-Data-breaches-hit-75-percent-of-all-US-adults/article/128281/>

• **Obama appoints federal CIO**

President Obama has appointed the first-ever federal chief information officer (CIO).

Vivek Kundra, 34, who formerly served in District of Columbia Mayor Adrian Fenty's cabinet as the chief technology officer (CTO) was appointed to the position, the White House announced Thursday.

"Vivek Kundra's technology leadership has greatly contributed to the administration's essential priority of building transparency, accountability and efficiency in government," Mayor Fenty told SCMagazineUS.com Thursday in an email. "I'm confident he'll be an equally great asset to the Obama Administration."

SC Magazine

Full Story :

<http://www.scmagazineus.com/Obama-appoints-federal-CIO/article/128347/>

New Vulnerabilities Tested in SecureScout

• 18281 VMware Workstation, Privilege escalation on 64-bit guest operating systems vulnerability (Remote File Checking)

VMware products emulate hardware functions, like CPU, Memory, and IO.

A flaw in VMware's CPU hardware emulation could allow the virtual CPU to jump to an incorrect memory address. Exploitation of this issue on the guest operating system does not lead to a compromise of the host system but could lead to a privilege escalation on guest operating system. An attacker would need to have a user account on the guest operating system.

Affected:

64-bit Windows and 64-bit FreeBSD guest operating systems and possibly other 64-bit operating systems. The issue does not affect the 64-bit versions of Linux guest operating systems.

The issue is fixed in VMware Workstation 5.5.8 build 108000 and VMware Workstation 6.0.5 build 109488.

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

References:

- * BUGTRAQ: 20081004 VMSA-2008-0016 VMware Hosted products, VirtualCenter Update 3 and <http://marc.info/?l=bugtraq&m=122331139823057&w=2>
- * BUGTRAQ: 20081004 VMSA-2008-0016 VMware Hosted products, VirtualCenter Update 3 and patches for ESX and ESXi resolve multiple security issues <http://www.securityfocus.com/archive/1/archive/1/497041/100/0/threaded>
- * FULLDISC: 20081004 VMware Emulation Flaw x64 Guest Privilege Escalation (1/2) <http://lists.grok.org.uk/pipermail/full-disclosure/2008-October/064860.html>
- * CONFIRM: <http://www.vmware.com/security/advisories/VMSA-2008-0016.html>
- * BID: 31569 <http://www.securityfocus.com/bid/31569>
- * OVAL: oval:org.mitre.oval:def:5929 <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5929>
- * NETVIGILANCE-UNKNOWN: ADV-2008-2740 <http://www.frsirt.com/english/advisories/2008/2740>
- * SECTrack: 1020991 <http://www.securitytracker.com/id?1020991>
- * SECUNIA: 32180 <http://secunia.com/advisories/32180>
- * SECUNIA: 32157 <http://secunia.com/advisories/32157>
- * SECUNIA: 32179 <http://secunia.com/advisories/32179>
- * XF: vmware-esxesxi-jump-privilege-escalation(45668) <http://xforce.iss.net/xforce/xfdb/45668>

CVE Reference:

CVE-2008-4279 (cve.mitre.org, nvd.nist.gov)

• 18282 VMware Server, Privilege escalation on 64-bit guest operating systems vulnerability (Remote File Checking)

VMware products emulate hardware functions, like CPU, Memory, and IO.

A flaw in VMware's CPU hardware emulation could allow the virtual CPU to jump to an incorrect memory address. Exploitation of this issue on the guest operating system does not lead to a compromise of the host system but could lead to a privilege escalation on guest operating system. An attacker would need to have a user account on the guest operating system.

Affected:

64-bit Windows and 64-bit FreeBSD guest operating systems and possibly other 64-bit operating systems. The issue does not affect the 64-bit versions of Linux guest operating systems.

The issue is fixed in VMware Server 1.0.7 build 108231.

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

References:

- * BUGTRAQ: 20081004 VMSA-2008-0016 VMware Hosted products, VirtualCenter Update 3 and <http://marc.info/?l=bugtraq&m=122331139823057&w=2>

* BUGTRAQ: 20081004 VMSA-2008-0016 VMware Hosted products, VirtualCenter Update 3 and patches for ESX and ESXi resolve multiple security issues
<http://www.securityfocus.com/archive/1/archive/1/497041/100/0/threaded>
* FULLDISC: 20081004 VMware Emulation Flaw x64 Guest Privilege Escalation (1/2)
<http://lists.grok.org.uk/pipermail/full-disclosure/2008-October/064860.html>
* CONFIRM:
<http://www.vmware.com/security/advisories/VMSA-2008-0016.html>
* BID: 31569
<http://www.securityfocus.com/bid/31569>
* OVAL: oval:org.mitre.oval:def:5929
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5929>
* NETVIGILANCE-UNKNOWN: ADV-2008-2740
<http://www.frsirt.com/english/advisories/2008/2740>
* SECTRAK: 1020991
<http://www.securitytracker.com/id?1020991>
* SECUNIA: 32180
<http://secunia.com/advisories/32180>
* SECUNIA: 32157
<http://secunia.com/advisories/32157>
* SECUNIA: 32179
<http://secunia.com/advisories/32179>
* XF: vmware-esxesxi-jump-privilege-escalation(45668)
<http://xforce.iss.net/xforce/xfdb/45668>

CVE Reference:

CVE-2008-4279 (cve.mitre.org, nvd.nist.gov)

• 18283 VMware Workstation, A privilege escalation on 32-bit and 64-bit guest operating systems vulnerability (Remote File Checking)

VMware products emulate hardware functions and create the possibility to run guest operating systems.

A flaw in the CPU hardware emulation might allow the virtual CPU to incorrectly handle the Trap flag. Exploitation of this flaw might lead to a privilege escalation on guest operating systems. An attacker needs a user account on the guest operating system and have the ability to run applications.

The issue is fixed in VMware Workstation 6.5.0 build 118166 and VMware Workstation 5.5.9 build 126128.

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

References:

* BUGTRAQ: 20081107 VMSA-2008-0018 VMware Hosted products and patches for ESX and ESXi resolve two security issues
<http://www.securityfocus.com/archive/1/archive/1/498138/100/0/threaded>
* MLIST: [Security-announce] 20081106 VMSA-2008-0018 VMware Hosted products and patches for ESX and ESXi resolve two security issues
<http://lists.vmware.com/pipermail/security-announce/2008/000042.html>
* CONFIRM:
<http://www.vmware.com/security/advisories/VMSA-2008-0018.html>
* BID: 32168
<http://www.securityfocus.com/bid/32168>
* NETVIGILANCE-UNKNOWN: ADV-2008-3052
<http://www.frsirt.com/english/advisories/2008/3052>
* SECTRAK: 1021154
<http://www.securitytracker.com/id?1021154>
* SECUNIA: 32612
<http://secunia.com/advisories/32612>
* SECUNIA: 32624
<http://secunia.com/advisories/32624>
* XF: vmware-cpuhardware-priv-escalation(46415)
<http://xforce.iss.net/xforce/xfdb/46415>

CVE Reference:

CVE-2008-4915 (cve.mitre.org, nvd.nist.gov)

• 18284 VMware Server, A privilege escalation on 32-bit and 64-bit guest operating systems vulnerability (Remote File Checking)

VMware products emulate hardware functions and create the possibility to run guest operating systems.

A flaw in the CPU hardware emulation might allow the virtual CPU to incorrectly handle the Trap flag. Exploitation of this flaw might lead to a privilege escalation on guest operating systems. An attacker needs a user account on the guest operating system and have the ability to run applications.

The issue is fixed in VMware Server 1.0.8 build 126538.

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

References:

- * BUGTRAQ: 20081107 VMSA-2008-0018 VMware Hosted products and patches for ESX and ESXi resolve two security issues
<http://www.securityfocus.com/archive/1/archive/1/498138/100/0/threaded>
- * MLIST: [Security-announce] 20081106 VMSA-2008-0018 VMware Hosted products and patches for ESX and ESXi resolve two security issues
<http://lists.vmware.com/pipermail/security-announce/2008/000042.html>
- * CONFIRM:
<http://www.vmware.com/security/advisories/VMSA-2008-0018.html>
- * BID: 32168
<http://www.securityfocus.com/bid/32168>
- * NETVIGILANCE-UNKNOWN: ADV-2008-3052
<http://www.frsirt.com/english/advisories/2008/3052>
- * SECTRACK: 1021154
<http://www.securitytracker.com/id?1021154>
- * SECUNIA: 32612
<http://secunia.com/advisories/32612>
- * SECUNIA: 32624
<http://secunia.com/advisories/32624>
- * XF: vmware-cpuhardware-priv-escalation(46415)
<http://xforce.iss.net/xforce/xfdb/46415>

CVE Reference:

CVE-2008-4915 (cve.mitre.org, nvd.nist.gov)

• 18285 VMware Workstation, Critical Memory corruption vulnerability (Remote File Checking)

A memory corruption condition may occur in the virtual machine hardware. A malicious request sent from the guest operating system to the virtual hardware may cause the virtual hardware to write to uncontrolled physical memory.

The issue is fixed in VMware Workstation 6.5.0 build 118166 and VMware Workstation 5.5.9 build 126128.

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

References:

- * BUGTRAQ: 20081203 Re: VMSA-2008-0019 VMware Hosted products and patches for ESX and ESXi resolve a critical security issue and update bzip2
<http://www.securityfocus.com/archive/1/archive/1/498886/100/0/threaded>
- * BUGTRAQ: 20081203 VMSA-2008-0019 VMware Hosted products and patches for ESX and ESXi resolve a critical security issue and update bzip2
<http://www.securityfocus.com/archive/1/archive/1/498863/100/0/threaded>
- * CONFIRM:
<http://kb.vmware.com/kb/1006980>
- * CONFIRM:
<http://kb.vmware.com/kb/1006986>
- * SECTRACK: 1021300
<http://securitytracker.com/id?1021300>
- * SECTRACK: 1021301
<http://securitytracker.com/id?1021301>
- * SECUNIA: 32965
<http://secunia.com/advisories/32965>

CVE Reference:

CVE-2008-4917 (cve.mitre.org, nvd.nist.gov)

• 18286 VMware Server, Critical Memory corruption vulnerability (Remote File Checking)

A memory corruption condition may occur in the virtual machine hardware. A malicious request sent from the guest operating system to the virtual hardware may cause the virtual hardware to write to uncontrolled physical memory.

The issue is fixed in VMware Server 1.0.8 build 126538.

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

References:

- * BUGTRAQ: 20081203 Re: VMSA-2008-0019 VMware Hosted products and patches for ESX and ESXi resolve a critical security issue and update bzip2
<http://www.securityfocus.com/archive/1/archive/1/498886/100/0/threaded>
- * BUGTRAQ: 20081203 VMSA-2008-0019 VMware Hosted products and patches for ESX and ESXi resolve a critical security issue and update bzip2
<http://www.securityfocus.com/archive/1/archive/1/498863/100/0/threaded>
- * CONFIRM:
<http://kb.vmware.com/kb/1006980>
- * CONFIRM:
<http://kb.vmware.com/kb/1006986>
- * SECTrack: 1021300
<http://securitytracker.com/id?1021300>
- * SECTrack: 1021301
<http://securitytracker.com/id?1021301>
- * SECUNIA: 32965
<http://secunia.com/advisories/32965>

CVE Reference:

CVE-2008-4917 (cve.mitre.org, nvd.nist.gov)

• 18288 Trillian AIM plugin heap-based buffer overflow Vulnerability (Remote File Checking)

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Cerulean Studios Trillian. Authentication is not required to exploit this vulnerability.

The specific flaw exists within the XML processing code for Trillian. When parsing a malformed XML tag, the application does not allocate enough space for its contents. During copying of this to the newly allocated buffer, the application will overwrite heap structures with attacker-supplied data that can then be leveraged to achieve code execution with the privileges of the application.

The vulnerability is reported fixed in version 3.1.12.0.

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

References:

- * BUGTRAQ: 20081205 ZDI-08-079: Trillian AIM Plugin Malformed XML Tag Heap Overflow Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/498936/100/0/threaded>
- * MISC:
<http://blog.ceruleanstudios.com/?p=404>
- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-08-079>
- * BID: 32645
<http://www.securityfocus.com/bid/32645>
- * NETVIGILANCE-UNKNOWN: ADV-2008-3348
<http://www.frsirt.com/english/advisories/2008/3348>
- * OSVDB: 50474
<http://osvdb.org/50474>
- * SECTrack: 1021336
<http://www.securitytracker.com/id?1021336>
- * SECUNIA: 33001
<http://secunia.com/advisories/33001>
- * SREASON: 4702
<http://securityreason.com/securityalert/4702>

CVE Reference:

CVE-2008-5403 (cve.mitre.org, nvd.nist.gov)

• 18289 Trillian IMG SRC ID Memory Corruption Vulnerability (Remote File Checking)

This vulnerability allows remote attackers to potentially execute arbitrary code on vulnerable installations of Cerulean Studios Trillian. Authentication is not required to exploit this vulnerability.

The specific flaw exists within the XML processing code for Trillian. When parsing specially formulated xml, the application will corrupt an internal data structure. Whilst deallocating this data structure, the application can be tricked into freeing a single allocated chunk multiple times, which can potentially lead to code execution.

The vulnerability is reported fixed in version 3.1.12.0.

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

References:

- * BUGTRAQ: 20081205 ZDI-08-078: Trillian IMG SRC ID Memory Corruption Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/498933/100/0/threaded>
- * MISC:
<http://blog.ceruleanstudios.com/?p=404>
- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-08-078>
- * BID: 32645
<http://www.securityfocus.com/bid/32645>
- * NETVIGILANCE-UNKNOWN: ADV-2008-3348
<http://www.frsirt.com/english/advisories/2008/3348>
- * OSVDB: 50473
<http://osvdb.org/50473>
- * SECTrack: 1021334
<http://www.securitytracker.com/id?1021334>
- * SECUNIA: 33001
<http://secunia.com/advisories/33001>
- * SREASON: 4701
<http://securityreason.com/securityalert/4701>
- * XF: trillian-xml-code-execution(47098)
<http://xforce.iss.net/xforce/xfdb/47098>

CVE Reference:

CVE-2008-5402 (cve.mitre.org, nvd.nist.gov)

• 18290 Trillian AIM IMG Tag Parsing Stack Overflow Vulnerability (Remote File Checking)

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Cerulean Studios Trillian. Authentication is not required to exploit this vulnerability.

The specific flaw exists within the tooltip processing code for Trillian. When creating a tooltip for an image, the application generates an XML tag including a property containing the filename. This data is then copied directly into a stack-based buffer without any length verifications which can eventually lead to code execution with the privileges of the client.

The vulnerability is reported fixed in version 3.1.12.0.

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

References:

- * BUGTRAQ: 20081205 ZDI-08-077: Trillian AIM IMG Tag Parsing Stack Overflow Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/498932/100/0/threaded>
- * MISC:
<http://blog.ceruleanstudios.com/?p=404>
- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-08-077>
- * BID: 32645
<http://www.securityfocus.com/bid/32645>
- * NETVIGILANCE-UNKNOWN: ADV-2008-3348
<http://www.frsirt.com/english/advisories/2008/3348>
- * OSVDB: 50472
<http://osvdb.org/50472>
- * SECTrack: 1021335
<http://www.securitytracker.com/id?1021335>
- * SECUNIA: 33001
<http://secunia.com/advisories/33001>
- * SREASON: 4700
<http://securityreason.com/securityalert/4700>
- * XF: trillian-xmltags-bo(47093)
<http://xforce.iss.net/xforce/xfdb/47093>

CVE Reference:

CVE-2008-5401 (cve.mitre.org, nvd.nist.gov)

• 18291 Winamp AIFF Processing Buffer Overflow Vulnerability (Remote File Checking)

Multiple buffer overflows in Winamp 5.541 and earlier allow remote attackers to cause a denial of service and possibly execute arbitrary code via a large Common Chunk (COMM) header value in an AIFF file and a large invalid value in an MP3 file.

The vulnerability is confirmed in version prior to 5.55.

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

References:

- * MILWORM: 7742
<http://milw0rm.com/exploits/7742>
- * BID: 33226
<http://www.securityfocus.com/bid/33226>
- * NETVIGILANCE-UNKNOWN: ADV-2009-0113
<http://www.frsirt.com/english/advisories/2009/0113>
- * SECUNIA: 33478
<http://secunia.com/advisories/33478>

CVE Reference:

CVE-2009-0263 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-0819 MySQL CVSS 2.0 Score = 5.0

sql/item_xmlfunc.cc in MySQL before 5.1.32 allows remote authenticated users to cause a denial of service (crash) via "an XPath expression employing a scalar expression as a FilterExpr with ExtractValue() or UpdateXML()," which triggers an assertion failure.

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

References:

- CONFIRM: <http://bugs.mysql.com/bug.php?id=42495>
- XF: <http://xforce.iss.net/xforce/xfdb/49050>
- VUPEN: <http://www.vupen.com/english/advisories/2009/0594>
- SECUNIA: <http://secunia.com/advisories/34115>
- CONFIRM: <http://dev.mysql.com/doc/refman/5.1/en/news-5-1-32.html>

CVE Reference: [CVE-2009-0819](#)

• CVE-2009-0779 IBM CVSS 2.0 Score = 7.2

Buffer overflow in pppdial in IBM AIX 5.3 and 6.1 allows local users to gain privileges via a long "input string."

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

References:

- VUPEN: <http://www.vupen.com/english/advisories/2009/0487>
- AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=isg1IZ44388>
- AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=isg1IZ44332>
- AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=isg1IZ44220>
- AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=isg1IZ44199>
- BID: <http://www.securityfocus.com/bid/33852>
- OSVDB: <http://www.osvdb.org/52179>
- SECTRAK: <http://securitytracker.com/id?1021741>

SECUNIA: <http://secunia.com/advisories/34005>

CVE Reference: [CVE-2009-0779](#)

• **CVE-2009-0619 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability in the Session Border Controller (SBC) before 3.0(2) for Cisco 7600 series routers allows remote attackers to cause a denial of service (SBC card reload) via crafted packets to TCP port 2000.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/49055>

BID: <http://www.securityfocus.com/bid/33975>

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080a80faa.shtml

CVE Reference: [CVE-2009-0619](#)

• **CVE-2009-0771 Mozilla CVSS 2.0 Score = 10.0**

The layout engine in Mozilla Firefox before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey 1.1.15 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via certain vectors that trigger memory corruption and assertion failures.

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

References:

CONFIRM:

https://bugzilla.mozilla.org/buglist.cgi?bug_id=424276,435209,436965,460706,466057,468578,471594,472502

CONFIRM: <http://www.mozilla.org/security/announce/2009/mfsa2009-07.html>

CVE Reference: [CVE-2009-0771](#)

• **CVE-2009-0773 Mozilla CVSS 2.0 Score = 10.0**

The JavaScript engine in Mozilla Firefox before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey 1.1.15 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via (1) a splice of an array that contains "some non-set elements," which causes jsarray.cpp to pass an incorrect argument to the ResizeSlots function, which triggers memory corruption; (2) vectors related to js_DecompileValueGenerator, jsopcode.cpp, __defineSetter__, and watch, which triggers an assertion failure or a segmentation fault; and (3) vectors related to gczeal, __defineSetter__, and watch, which triggers a hang.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=472787

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=467499

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=457521

CONFIRM: <http://www.mozilla.org/security/announce/2009/mfsa2009-07.html>

CVE Reference: [CVE-2009-0773](#)

• **CVE-2009-0775 Mozilla CVSS 2.0 Score = 10.0**

Double free vulnerability in Mozilla Firefox before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey before 1.1.15 allows remote attackers to execute arbitrary code via "cloned XUL DOM elements which were linked as a parent and child," which are not properly handled during garbage collection.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=474456

CONFIRM: <http://www.mozilla.org/security/announce/2009/mfsa2009-08.html>

CVE Reference: [CVE-2009-0775](#)

• **CVE-2009-0772 Mozilla CVSS 2.0 Score = 9.3**

The layout engine in Mozilla Firefox 2 and 3 before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey 1.1.15 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to nsCSSStyleSheet::GetOwnerNode, events, and garbage collection, which triggers memory corruption.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=475136

CONFIRM: <http://www.mozilla.org/security/announce/2009/mfsa2009-07.html>

CVE Reference: [CVE-2009-0772](#)

• **CVE-2009-0774 Mozilla CVSS 2.0 Score = 9.3**

The layout engine in Mozilla Firefox 2 and 3 before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey 1.1.15 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to gczeal, a different vulnerability than CVE-2009-0773.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=473709

CONFIRM: <http://www.mozilla.org/security/announce/2009/mfsa2009-07.html>

CVE Reference: [CVE-2009-0774](#)

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