netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 9

March 2, 2007

Table of Contents

Product Focus

Messenger Service Vulnerability Scanner – The Messenger Service 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 Microsoft Windows Messenger Service flaw (MS03-043).

netVigilance free Single Scanners now support Windows XP Sp2. For a full list and download, go to http://www.netvigilance.com/singlescanners

netvigilance announces support for Delta Reports in SecureScout SP.

This Week in Review

A look at malware in 2006. The feds work with businesses. Read some visions on computers and the environment. What about malware in hardware.

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

- **Targeted malware rises once again**

The number of new malicious programs in 2006 rose by 41 per cent on the previous year's figures, according to vendor Kasperksy Lab's annual report.

The number of Trojans analysed by the Kaspersky Lab in 2006 far outweighed the number of worms, continuing the trend from previous years.

'New families of Trojans and variants accounted for 90 per cent of all new malware last year. This is attributable to the fact they are relatively easy to write and can be used to steal information, create botnets and execute mass spam mailings,' said Alex Gostev, senior virus analyst at Kaspersky Lab.

In 2006, there was a clear increase in malicious programs for areas previously thought to be relatively secure, such as online games and social networking sites.

Due to the lack of critical vulnerabilities in Microsoft Windows system services, hackers and other malicious users turned their attention to other popular software products according to the report.

vnunet

Full Story :
http://www.vnunet.com/computing/news/2184637/malware-rises-41-per-cent

❖ Feds hope to boost business role in slowing cyberattacks

As reports of cybersecurity incidents grow, U.S. Department of Homeland Security officials plan to improve their ability to work on the problem face to face with private-sector experts.

The DHS plans to collocate private-sector employees from the communications and IT industries with government workers at the U.S. Computer Emergency Readiness Team (US-CERT) facility here, said Gregory Garcia, assistant secretary of cybersecurity and telecommunications at the DHS. The teams will work jointly on improving US-CERT's information hub for cybersecurity, Garcia said. The agency didn't specify a starting date for the program but said it will begin soon.

US-CERT is a four-year-old DHS-run joint effort of the public and private sectors to protect the nation's Internet infrastructure. "It's through this collocation that we are going to build a strong trust relationship, an information-sharing relationship," said Garcia.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9012132&taxonomyId=17&intsrc=kc_top

❖ Only IT can save the world

Once upon a time, I was a member of the Green Party. I went as far as standing for a local council seat in East London, in a part of town where the only green thing was the meat in the dodgier kebab shops. My experience of polling day was surprisingly similar to eating one of those kebabs — it taught me a lot about expectation and reality, and the consequences of trusting appearance without questioning content.

I get much the same visceral reaction when I read many of the press releases that pollute my inbox. Companies big and small are only too happy to cloak themselves in earth-friendly camouflage, for all sorts of reasons. None of it's worth a single sheet of recyclable toilet paper without evidence that they've understood and bought into the real philosophy of environmental thinking — so expect a lot more scepticism from this website.

The real irony is that IT has the potential to transform itself into the most environmentally sound industry on the planet. More than in any other area of human activity, the science that lies behind our technology is capable of driving revolutionary changes in the way we work, without impacting on the effectiveness of what we do. The creation, distribution and consumption of material goods will be forever in thrall to Newton's laws of matter and energy: information, however, is different.

zdnet

Full Story :
http://opinion.zdnet.co.uk/comment/0,1000002138,39286147,00.htm

- **PC hardware can pose rootkit threat**

ARLINGTON, Va.--PC hardware components can provide a way for hackers to sneak malicious code onto a computer, a security researcher warned Wednesday.

Every component in a PC, such as graphics cards, DVD drives and batteries, has some memory space for the software that runs it, called firmware. Miscreants could use this space to hide malicious code that would load the next time the PC boots, John Heasman, research director at NGS Software, said in a presentation at this week's Black Hat DC event here.

"This is an important area and people should be concerned about this," Heasman said. "Software security is getting better, yet we run increasingly complicated hardware. Unless we address hardware security, we're leaving an interesting avenue for attack."

zdnet

Full Story :
http://news.zdnet.com/2100-1009_22-6162924.html

New Vulnerabilities Tested in SecureScout

- **16437 Linux Kernel NFSACL "ACCESS" Denial of Service**

A vulnerability has been reported in the Linux Kernel, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an invalid freeing of a pointer when handling NFSACL 2 "ACCESS" requests, which can be exploited to crash the kernel.

The vulnerability is reported in version prior to 2.6.20.1

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.20.1

Other references:
* FRSIRT:ADV-2007-0660
* URL:http://www.frsirt.com/english/advisories/2007/0660
* SECUNIA:24215
* URL:http://secunia.com/advisories/24215

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2007-0772

❖ 16440 Mozilla Firefox Network Security Services, integer underflow Vulnerability (Remote File Checking)

A vulnerability has been reported in Mozilla Firefox, which can be exploited by malicious people to potentially compromise a user's system.

An integer underflow error in the Network Security Services (NSS) code when processing SSLv2 server messages can be exploited to cause a heap-based buffer overflow via a certificate with a public key too small to encrypt the "Master Secret".

Successful exploitation may allow execution of arbitrary code.

NOTE: Support for SSLv2 is disabled in Firefox 2.x. This version is only vulnerable if user has modified hidden internal NSS settings to re-enable SSLv2 support.

The weakness is confirmed in version 2.0.0.1 and 1.5.0.9. Other versions may also be affected.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2007/mfsa2007-06.html

Other references:
IDEFENSE:20070223 Mozilla Network Security Services SSLv2 Client Integer Underflow Vulnerability
URL:http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=482
MISC: https://bugzilla.mozilla.org/show_bug.cgi?id=364319

FEDORA:FEDORA-2007-278
URL:http://fedoranews.org/cms/node/2709
FEDORA:FEDORA-2007-279
URL:http://fedoranews.org/cms/node/2711
FEDORA:FEDORA-2007-281
URL:http://fedoranews.org/cms/node/2713
REDHAT:RHSA-2007:0079
URL:http://www.redhat.com/support/errata/RHSA-2007-0079.html
REDHAT:RHSA-2007:0077
URL:http://rhn.redhat.com/errata/RHSA-2007-0077.html
UBUNTU:USN-428-1
URL:http://www.ubuntu.com/usn/usn-428-1
BID:22694
URL:http://www.securityfocus.com/bid/22694
FRSIRT:ADV-2007-0719
URL:http://www.frsirt.com/english/advisories/2007/0719
FRSIRT:ADV-2007-0718
URL:http://www.frsirt.com/english/advisories/2007/0718
SECTRACK:1017696
URL:http://www.securitytracker.com/id?1017696
SECUNIA:24238
URL:http://secunia.com/advisories/24238
SECUNIA:24252
URL:http://secunia.com/advisories/24252
SECUNIA:24253
URL:http://secunia.com/advisories/24253
SECUNIA:24277
URL:http://secunia.com/advisories/24277
SECUNIA:24287
URL:http://secunia.com/advisories/24287
SECUNIA:24290
URL:http://secunia.com/advisories/24290
SECUNIA:24205
URL:http://secunia.com/advisories/24205
SECUNIA:24328
URL:http://secunia.com/advisories/24328
XF:nss-mastersecret-bo(32666)
URL:http://xforce.iss.net/xforce/xfdb/32666

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2007-0008

❖ 16441 Mozilla Firefox frame with a "data:", cross-site scripting Vulnerability (Remote File Checking)

A vulnerability has been reported in Mozilla Firefox, which can be exploited by malicious people to conduct cross-site scripting attacks.

It is possible to conduct cross-site scripting attacks against sites containing a frame with a "data:" URI as source.

Successful exploitation requires that a user is tricked into visiting a malicious website and opening a blocked popup.

The weakness is confirmed in version 2.0.0.1 and 1.5.0.9. Other versions may also be affected.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2007/mfsa2007-05.html

Other references:
MISC: https://bugzilla.mozilla.org/show_bug.cgi?id=354973
FEDORA:FEDORA-2007-281
URL:http://fedoranews.org/cms/node/2713
REDHAT:RHSA-2007:0079
URL:http://www.redhat.com/support/errata/RHSA-2007-0079.html
REDHAT:RHSA-2007:0077
URL:http://rhn.redhat.com/errata/RHSA-2007-0077.html
UBUNTU:USN-428-1
URL:http://www.ubuntu.com/usn/usn-428-1
BID:22694
URL:http://www.securityfocus.com/bid/22694
FRSIRT:ADV-2007-0718
URL:http://www.frsirt.com/english/advisories/2007/0718
SECTRACK:1017702
URL:http://www.securitytracker.com/id?1017702
SECUNIA:24238
URL:http://secunia.com/advisories/24238
SECUNIA:24287
URL:http://secunia.com/advisories/24287
SECUNIA:24290
URL:http://secunia.com/advisories/24290
SECUNIA:24205
URL:http://secunia.com/advisories/24205
SECUNIA:24328
URL:http://secunia.com/advisories/24328
XF:mozilla-dataurl-xss(32667)
URL:http://xforce.iss.net/xforce/xfdb/32667

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2007-0780

❖ 16442 Mozilla Firefox CSS3 hotspot property manipulation Vulnerability (Remote File Checking)

A vulnerability has been reported in Mozilla Firefox, which can be exploited by malicious people to spoof some of the browser elements.

Browser UI elements like the host name and security indicators can be spoofed using a specially crafted custom cursor and manipulating the CSS3 hotspot property.

The weakness is confirmed in version 2.0.0.1 and 1.5.0.9. Other versions may also be affected.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2007/mfsa2007-04.html

Other references:
MISC: https://bugzilla.mozilla.org/show_bug.cgi?id=361298
FEDORA:FEDORA-2007-281
URL:http://fedoranews.org/cms/node/2713
REDHAT:RHSA-2007:0079
URL:http://www.redhat.com/support/errata/RHSA-2007-0079.html
REDHAT:RHSA-2007:0077
URL:http://rhn.redhat.com/errata/RHSA-2007-0077.html
UBUNTU:USN-428-1
URL:http://www.ubuntu.com/usn/usn-428-1
BID:22694
URL:http://www.securityfocus.com/bid/22694
FRSIRT:ADV-2007-0718
URL:http://www.frsirt.com/english/advisories/2007/0718
SECTRACK:1017700
URL:http://www.securitytracker.com/id?1017700
SECUNIA:24238
URL:http://secunia.com/advisories/24238
SECUNIA:24287
URL:http://secunia.com/advisories/24287
SECUNIA:24290
URL:http://secunia.com/advisories/24290
SECUNIA:24205
URL:http://secunia.com/advisories/24205
SECUNIA:24328
URL:http://secunia.com/advisories/24328

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2007-0779

❖ 16443 Mozilla Firefox web pages colliding in the disk cache Vulnerability (Remote File Checking)

A vulnerability has been reported in Mozilla Firefox, which can be exploited by malicious people to gain knowledge of sensitive information.

It may be possible to gain knowledge of sensitive information from a website due to

an error resulting in two web pages colliding in the disk cache thereby potentially appending part of one document to the other.

Successful exploitation requires that a user is tricked into visiting a malicious website while visiting the target website.

The weakness is confirmed in version 2.0.0.1 and 1.5.0.9. Other versions may also be affected.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2007/mfsa2007-03.html

Other references:
MISC: https://bugzilla.mozilla.org/show_bug.cgi?id=347852
FEDORA:FEDORA-2007-281
URL:http://fedoranews.org/cms/node/2713
REDHAT:RHSA-2007:0079
URL:http://www.redhat.com/support/errata/RHSA-2007-0079.html
REDHAT:RHSA-2007:0077
URL:http://rhn.redhat.com/errata/RHSA-2007-0077.html
UBUNTU:USN-428-1
URL:http://www.ubuntu.com/usn/usn-428-1
BID:22694
URL:http://www.securityfocus.com/bid/22694
FRSIRT:ADV-2007-0718
URL:http://www.frsirt.com/english/advisories/2007/0718
SECTRACK:1017699
URL:http://securitytracker.com/id?1017699
SECUNIA:24238
URL:http://secunia.com/advisories/24238
SECUNIA:24287
URL:http://secunia.com/advisories/24287
SECUNIA:24290
URL:http://secunia.com/advisories/24290
SECUNIA:24205
URL:http://secunia.com/advisories/24205
SECUNIA:24328
URL:http://secunia.com/advisories/24328
XF:mozilla-diskcache-information-disclosure(32671)
URL:http://xforce.iss.net/xforce/xfdb/32671

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2007-0778

❖ **16444 Mozilla Firefox processing of UTF-7 and handling invalid trailing characters in HTML tag attribute names Vulnerabilities (Remote File Checking)**

Some vulnerabilities have been reported in Mozilla Firefox, which can be exploited by malicious people to conduct cross-site scripting attacks.

Various errors in the Mozilla parser when handling invalid trailing characters in HTML tag attribute names and during processing of UTF-7 content when child frames inherit the character set of its parent window can be exploited to conduct cross-site scripting attacks.

The weakness is confirmed in version 2.0.0.1 and 1.5.0.9. Other versions may also be affected.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2007/mfsa2007-02.html

Other references:
MISC: http://ha.ckers.org/xss.html#XSS_Non_alpha_non_digit2
FEDORA:FEDORA-2007-281
URL:http://fedoranews.org/cms/node/2713
REDHAT:RHSA-2007:0079
URL:http://www.redhat.com/support/errata/RHSA-2007-0079.html
REDHAT:RHSA-2007:0077
URL:http://rhn.redhat.com/errata/RHSA-2007-0077.html
UBUNTU:USN-428-1
URL:http://www.ubuntu.com/usn/usn-428-1
BID:22694
URL:http://www.securityfocus.com/bid/22694
FRSIRT:ADV-2007-0718
URL:http://www.frsirt.com/english/advisories/2007/0718
SECTRACK:1017702
URL:http://www.securitytracker.com/id?1017702
SECUNIA:24238
URL:http://secunia.com/advisories/24238
SECUNIA:24287
URL:http://secunia.com/advisories/24287
SECUNIA:24290
URL:http://secunia.com/advisories/24290
SECUNIA:24205
URL:http://secunia.com/advisories/24205
SECUNIA:24328
URL:http://secunia.com/advisories/243287

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2007-0995

❖ **16445 Mozilla Firefox vulnerability in the Password Manager Vulnerability (Remote File Checking)**

Some vulnerabilities have been reported in Mozilla Firefox, which can be exploited by malicious people to conduct phishing attacks.

A vulnerability in the Password Manager may be exploited to conduct phishing attacks.

The weakness is confirmed in version 2.0.0.1 and 1.5.0.9. Other versions may also be affected.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2007/mfsa2007-02.html

Other references:
BUGTRAQ:20061122 Big Flaw in Firefox 2: Password Manager Bug Exposes Passwords
URL:http://www.securityfocus.com/archive/1/archive/1/452382/100/0/threaded
BUGTRAQ:20061123 Password Flaw also in Firefox 1.5.08. Was: Big Flaw in Firefox 2: Password Manager Bug Exposes Passwords
URL:http://www.securityfocus.com/archive/1/archive/1/452431/100/0/threaded
BUGTRAQ:20061123 Re: Big Flaw in Firefox 2: Password Manager Bug Exposes Passwords
URL:http://www.securityfocus.com/archive/1/archive/1/452440/100/0/threaded
BUGTRAQ:20061123 Re: Password Flaw also in Firefox 1.5.08. Was: Big Flaw in Firefox 2: Password Manager Bug Exposes Passwords
URL:http://www.securityfocus.com/archive/1/archive/1/452463/100/0/threaded
BUGTRAQ:20061220 critical Flaw in Firefox 2.0.0.1 allows to steal the user passwords with a videoclip
URL:http://www.securityfocus.com/archive/1/archive/1/454982/100/0/threaded
BUGTRAQ:20061221 Re: critical Flaw in Firefox 2.0.0.1 allows to steal the user passwords with a videoclip
URL:http://www.securityfocus.com/archive/1/archive/1/455073/100/0/threaded
BUGTRAQ:20061222 Re[2]: critical Flaw in Firefox 2.0.0.1 allows to steal the user passwords with a videoclip
URL:http://www.securityfocus.com/archive/1/archive/1/455148/100/0/threaded
MISC: http://www.info-svc.com/news/11-21-2006/
MISC: http://www.info-svc.com/news/11-21-2006/rcsr1/
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=360493
FEDORA:FEDORA-2007-281
URL:http://fedoranews.org/cms/node/2713
REDHAT:RHSA-2007:0079
URL:http://www.redhat.com/support/errata/RHSA-2007-0079.html
REDHAT:RHSA-2007:0077
URL:http://rhn.redhat.com/errata/RHSA-2007-0077.html
UBUNTU:USN-428-1
URL:http://www.ubuntu.com/usn/usn-428-1
BID:21240
URL:http://www.securityfocus.com/bid/21240
BID:22694
URL:http://www.securityfocus.com/bid/22694
FRSIRT:ADV-2006-4662
URL:http://www.frsirt.com/english/advisories/2006/4662

FRSIRT:ADV-2007-0718
URL:http://www.frsirt.com/english/advisories/2007/0718
SECTRACK:1017271
URL:http://securitytracker.com/id?1017271
SECUNIA:23046
URL:http://secunia.com/advisories/23046
SECUNIA:23108
URL:http://secunia.com/advisories/23108
SECUNIA:24238
URL:http://secunia.com/advisories/24238
SECUNIA:24287
URL:http://secunia.com/advisories/24287
SECUNIA:24290
URL:http://secunia.com/advisories/24290
SECUNIA:24205
URL:http://secunia.com/advisories/24205
SECUNIA:24328
URL:http://secunia.com/advisories/24328
XF:firefox-passwordmgr-information-disclosure(30470)
URL:http://xforce.iss.net/xforce/xfdb/30470

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-6077

❖ 16446 Mozilla Firefox layout engine, JavaScript engine, and in SVG, multiple memory corruption errors Vulnerability (Remote File Checking)

Some vulnerabilities have been reported in Mozilla Firefox, which can be exploited by malicious people to execute arbitrary code on a user's system.

Multiple memory corruption errors exist in the layout engine, JavaScript engine, and in SVG. Some of these may be exploited to execute arbitrary code on a user's system.

The weakness is confirmed in version 2.0.0.1 and 1.5.0.9. Other versions may also be affected.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2007/mfsa2007-01.html

Other references:
FEDORA:FEDORA-2007-281
URL:http://fedoranews.org/cms/node/2713
REDHAT:RHSA-2007:0079
URL:http://www.redhat.com/support/errata/RHSA-2007-0079.html
REDHAT:RHSA-2007:0077
URL:http://rhn.redhat.com/errata/RHSA-2007-0077.html

UBUNTU:USN-428-1
URL:http://www.ubuntu.com/usn/usn-428-1
BID:22694
URL:http://www.securityfocus.com/bid/22694
FRSIRT:ADV-2007-0719
URL:http://www.frsirt.com/english/advisories/2007/0719
FRSIRT:ADV-2007-0718
URL:http://www.frsirt.com/english/advisories/2007/0718
SECTRACK:1017698
URL:http://www.securitytracker.com/id?1017698
SECUNIA:24238
URL:http://secunia.com/advisories/24238
SECUNIA:24252
URL:http://secunia.com/advisories/24252
SECUNIA:24287
URL:http://secunia.com/advisories/24287
SECUNIA:24290
URL:http://secunia.com/advisories/24290
SECUNIA:24205
URL:http://secunia.com/advisories/24205
SECUNIA:24328
URL:http://secunia.com/advisories/24328

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2007-0775

❖ 16447 Mozilla Firefox handling of onUnload event handler, and self-modifying document.write() calls, code execution Vulnerability (Remote File Checking)

Some vulnerabilities have been reported in Mozilla Firefox, which can be exploited by malicious people to execute arbitrary code on a user's system.

An error within the handling of the onUnload event handler and self-modifying document.write() calls can be exploited to corrupt memory and potentially execute arbitrary code.

The weakness is confirmed in version 2.0.0.1 and 1.5.0.9. Other versions may also be affected.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2007/mfsa2007-08.html

Other references:
BUGTRAQ:20070223 Firefox onUnload + document.write() memory corruption vulnerability (MSIE7 null ptr)
URL:http://www.securityfocus.com/archive/1/archive/1/461024/100/0/threaded

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=371321
UBUNTU:USN-428-1
URL:http://www.ubuntu.com/usn/usn-428-1
CERT-VN:VU#393921
URL:http://www.kb.cert.org/vuls/id/393921
BID:22679
URL:http://www.securityfocus.com/bid/22679
SECTRACK:1017701
URL:http://www.securitytracker.com/id?1017701
XF:mozilla-onunload-code-execution(32648)
URL:http://xforce.iss.net/xforce/xfdb/32648

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2007-1092

❖ 16448 Mozilla Firefox opening windows containing local files Vulnerability (Remote File Checking)

Some vulnerabilities have been reported in Mozilla Firefox, which can be exploited by malicious people to disclose sensible information.

It is possible to open windows containing local files thereby stealing the contents when the full path of a locally saved file containing malicious script code is known. This can be exploited in combination with a flaw in the seeding of the pseudo-random number generator causing downloaded files to be saved to temporary files with a somewhat predictable name.

Successful exploitation requires that a user is tricked into visiting a malicious website and opening a blocked popup.

The weakness is confirmed in version 2.0.0.1 and 1.5.0.9. Other versions may also be affected.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2007/mfsa2007-05.html

Other references:
BUGTRAQ:20070205 Firefox + popup blocker + XMLHttpRequest + srand() = oops
#
URL:http://www.securityfocus.com/archive/1/archive/1/459162/100/0/threaded
BUGTRAQ:20070205 Re: [Full-disclosure] Firefox + popup blocker + XMLHttpRequest + srand() = oops
URL:http://www.securityfocus.com/archive/1/459163/100/0/threaded
FULLDISC:20070205 Firefox + popup blocker + XMLHttpRequest + srand() = oops
URL:http://lists.grok.org.uk/pipermail/full-disclosure/2007-February/052209.html
FULLDISC:20070205 Re: Firefox + popup blocker + XMLHttpRequest + srand() = oops

URL:http://lists.grok.org.uk/pipermail/full-disclosure/2007-February/052211.html
CONFIRM: http://www.mozilla.org/security/announce/2007/mfsa2007-05.html
FEDORA:FEDORA-2007-281
URL:http://fedoranews.org/cms/node/2713
REDHAT:RHSA-2007:0079
URL:http://www.redhat.com/support/errata/RHSA-2007-0079.html
REDHAT:RHSA-2007:0077
URL:http://rhn.redhat.com/errata/RHSA-2007-0077.html
UBUNTU:USN-428-1
URL:http://www.ubuntu.com/usn/usn-428-1
BID:22396
URL:http://www.securityfocus.com/bid/22396
BID:22694
URL:http://www.securityfocus.com/bid/22694
FRSIRT:ADV-2007-0718
URL:http://www.frsirt.com/english/advisories/2007/0718
SECTRACK:1017702
URL:http://www.securitytracker.com/id?1017702
SECUNIA:24238
URL:http://secunia.com/advisories/24238
SECUNIA:24287
URL:http://secunia.com/advisories/24287
SECUNIA:24290
URL:http://secunia.com/advisories/24290
SECUNIA:24205
URL:http://secunia.com/advisories/24205
SECUNIA:24328
URL:http://secunia.com/advisories/24328
XF:firefox-popup-security-bypass(32194)
URL:http://xforce.iss.net/xforce/xfdb/32194

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2007-0800

New Vulnerabilities found this Week

Mozilla Firefox Multiple Vulnerabilities

"Bypass security restrictions; conduct cross-site scripting; spoofing attacks; gain knowledge of sensitive information, and potentially compromise a user's system"

Multiple vulnerabilities have been reported in Mozilla Firefox, which can be exploited by malicious people to bypass certain security restrictions, conduct cross-site scripting and spoofing attacks, gain knowledge of sensitive information, and potentially compromise a user's system.

1) An error in the handling of the "locations.hostname" DOM property can be exploited to bypass certain security restrictions.

2) An integer underflow error in the Network Security Services (NSS) code when processing SSLv2 server messages can be exploited to cause a heap-based buffer

overflow via a certificate with a public key too small to encrypt the "Master Secret".

Successful exploitation may allow execution of arbitrary code.

NOTE: Support for SSLv2 is disabled in Firefox 2.x. This version is only vulnerable if user has modified hidden internal NSS settings to re-enable SSLv2 support.

3) It is possible to conduct cross-site scripting attacks against sites containing a frame with a "data:" URI as source.

Successful exploitation requires that a user is tricked into visiting a malicious website and opening a blocked popup.

4) It is possible to open windows containing local files thereby stealing the contents when the full path of a locally saved file containing malicious script code is known. This can be exploited in combination with a flaw in the seeding of the pseudo-random number generator causing downloaded files to be saved to temporary files with a somewhat predictable name.

Successful exploitation requires that a user is tricked into visiting a malicious website and opening a blocked popup.

5) Browser UI elements like the host name and security indicators can be spoofed using a specially crafted custom cursor and manipulating the CSS3 hotspot property.

6) It may be possible to gain knowledge of sensitive information from a website due to an error resulting in two web pages colliding in the disk cache thereby potentially appending part of one document to the other.

Successful exploitation requires that a user is tricked into visiting a malicious website while visiting the target website.

7) Various errors in the Mozilla parser when handling invalid trailing characters in HTML tag attribute names and during processing of UTF-7 content when child frames inherit the character set of its parent window can be exploited to conduct cross-site scripting attacks.

8) A vulnerability in the Password Manager may be exploited to conduct phishing attacks.

9) Multiple memory corruption errors exist in the layout engine, JavaScript engine, and in SVG. Some of these may be exploited to execute arbitrary code on a user's system.

10) An error within the handling of the onUnload event handler and self-modifying document.write() calls can be exploited to corrupt memory and potentially execute arbitrary code.

References:
http://www.mozilla.org/security/announce/2007/mfsa2007-08.html
http://www.mozilla.org/security/announce/2007/mfsa2007-07.html
http://www.mozilla.org/security/announce/2007/mfsa2007-06.html
http://www.mozilla.org/security/announce/2007/mfsa2007-05.html
http://www.mozilla.org/security/announce/2007/mfsa2007-04.html
http://www.mozilla.org/security/announce/2007/mfsa2007-03.html
http://www.mozilla.org/security/announce/2007/mfsa2007-02.html

http://www.mozilla.org/security/announce/2007/mfsa2007-01.html
http://descriptions.securescout.com/tc/16440
http://descriptions.securescout.com/tc/16441
http://descriptions.securescout.com/tc/16442
http://descriptions.securescout.com/tc/16443
http://descriptions.securescout.com/tc/16444
http://descriptions.securescout.com/tc/16445
http://descriptions.securescout.com/tc/16446
http://descriptions.securescout.com/tc/16447
http://descriptions.securescout.com/tc/16448

Internet Explorer 7 "onunload" Event Spoofing Vulnerability

"Spoof the address bar"

Secunia Research has discovered a vulnerability in Internet Explorer 7, which can be exploited by a malicious website to spoof the address bar.

The vulnerability is caused due to an error in Internet Explorer 7's handling of "onunload" events, enabling a malicious website to abort the loading of a new website. This can be exploited to spoof the address bar if e.g. the user enters a new website manually in the address bar, which is commonly exercised as best practice.

The vulnerability is confirmed on a fully patched Windows XP SP2 system running Internet Explorer 7. Other versions may also be affected.

References:
http://secunia.com/secunia_research/2007-1/

Network Security Services SSLv2 Processing Buffer Overflows

"Execution of arbitrary code"

Two vulnerabilities have been reported in Network Security Services (NSS), which potentially can be exploited by malicious people to compromise a vulnerable system.

1) An integer underflow error when processing SSLv2 server messages can be exploited to cause a heap-based buffer overflow via a certificate with a public key too small to encrypt the "Master Secret".

2) An integer underflow error when processing SSLv2 client master keys can be exploited to cause a stack-based buffer overflow via specially crafted parameters during an SSLv2 handshake.

Successful exploitation of the vulnerabilities may allow execution of arbitrary code.

The vulnerabilities are reported in versions 3.10 and 3.11.3. Other versions may also be affected.

References:
http://www.mozilla.org/security/announce/2007/mfsa2007-06.html
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=482
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=483

Microsoft Windows Directory Monitoring Information Disclosure Weakness
"Gain knowledge of certain information"

3APA3A has discovered a weakness in Microsoft Windows, which can be exploited by malicious, local users to gain knowledge of certain information.

The problem is caused due to the "ReadDirectoryChangesW()" API not taking into consideration the permissions of sub-directories when monitoring directories. This can be exploited to e.g. disclose file names in protected sub-directories.

Successful exploitation requires that the protected files are in a sub-directory where the parent directory is accessible by the attacker.

The weakness is confirmed on fully-patched Windows XP SP2 and Windows Server 2003 systems. Microsoft Windows 2000 and Vista are also reported to be affected.

References:
http://lists.grok.org.uk/pipermail/full-disclosure/2007-February/052613.html

VeriSign ConfigChk ActiveX Control Buffer Overflow
"Execution of arbitrary code"

David D. Rude II has reported a vulnerability in VeriSign's ConfigChk ActiveX control, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the ConfigChk ActiveX control (VSCnfChk.dll) when processing arguments passed to the VerCompare() method. This can be exploited to cause a stack-based based buffer overflow via an overly long (greater than 28 bytes) string passed as argument to the said method.

Successful exploitation allows execution of arbitrary code but requires that the user is e.g. tricked into visiting a malicious web site.

The vulnerability is reported in version 2.0.0.2. Other versions may also be affected.

References:
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=479

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