netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 36

September 14, 2007

Table of Contents

Product Focus

Sasser Worm Scanner – The Sasser Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Microsoft SSL Vulnerability (MS04-011) that used by the Sasser Worm to infect machines.

This Week in Review

One software vendor forces users to upgrade. Another leads a charge for internet privacy standards. And EU is pondering about internet censoring. A look at security spendings.

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

- **Microsoft forces MSN Messenger upgrade for 'security' reasons**

'To protect you and the health of the network'
Microsoft is forcing Windows Live and MSN Messenger users to upgrade to the newest version because of a security update included in that release, according to a posting on a Microsoft blog.

Anyone using 6.2, 7.0 and 7.5 versions of MSN Messenger or Windows Live Messenger

8.0 will be guided through the upgrade process to Windows Live Messenger 8.1 when they try to log into their chat client, according to a blog posting by a security product manager at Microsoft calling himself Anand. This will replace the option upgrade notice that users have been given when using those versions of the product since January, he wrote.

PCAdvisor

Full Story :
http://www.pcadvisor.co.uk/news/index.cfm?newsid=10731

❖ Google proposes global privacy standard

While Google is leading a charge to create a global privacy standard for how companies protect consumer data, the search giant is recommending that remedies focus on whether a person was actually harmed by having the information exposed.

Google's proposal is scheduled to be presented by Peter Fleischer, Google's global privacy counsel in a speech Friday in Strasbourg, France, at UNESCO's meeting on ethics and human rights. He briefed reporters on Thursday.

The proposal follows the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, which has been endorsed by many of the APEC nations, including Australia and Hong Kong, but not all. China, for instance, does not endorse it, Fleischer said.

cnet

Full Story :
http://www.news.com/Google+proposes+global+privacy+standard/2100-1030_3-6207927.html?tag=newsmap

❖ The internet should be censored for security

Internet service providers should block searches for bomb-making instructions, according to the EU's top security official.

Franco Frattini, EU Justice and Security Commissioner, this week told Reuters (see useful links) that freedom of information should come second to security and that sites that could help terrorists in bomb-making and other security issues should be blocked across the EU.

He told Reuters: "I intend to carry out a clear exploring exercise with the private sector on how it is possible to use technology to prevent people from using or searching dangerous words like 'bomb', 'kill', 'genocide' or 'terrorism'.

Broadband Choices

Full Story :
http://www.broadbandchoices.co.uk/the-internet-should-be-censored-for-security-130907.html

- **Antivirus is biggest security expense**

Spending on security software across Europe will top €2.4bn (£1.65bn) this year, with antivirus continuing to form the largest slice of the pie.

Antivirus will account for more than 50 percent of the total security software revenue market in 2007, according to the calculations by analyst Gartner.
Organisations are getting more sophisticated in the way they choose security products, and technical evaluations are now common practice, the analyst said. Customers also want to deal with a smaller number of vendors that can supply products that work well together.

zdnet

Full Story :
http://news.zdnet.co.uk/security/0,1000000189,39289294,00.htm

New Vulnerabilities Tested in SecureScout

- **16623 Mozilla Firefox - Arbitrary code execution via crafted XPCNativeWrapper (Remote File Checking)**

Multiple unspecified vulnerabilities in Mozilla Firefox before 2.0.0.5 allow remote attackers to execute arbitrary code via a crafted XPCNativeWrapper.

The issue has been fixed in Firefox 2.0.0.5.

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

References:

* BUGTRAQ: 20070720 rPSA-2007-0148-1 firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/474226/100/0/threaded
* BUGTRAQ: 20070724 FLEA-2007-0033-1: firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/474542/100/0/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-25.html
* CONFIRM:
ftp://ftp.slackware.com/pub/slackware/slackware-12.0/ChangeLog.txt
* CONFIRM:
http://support.novell.com/techcenter/psdb/07d098f99c9fe6956523beae37f32fda.html

CVE Reference: CVE-2007-3738

- **16622 Mozilla Firefox - Arbitrary code execution with chrome privileges by calling an event handler from an unspecified "element outside of a document." (Remote File Checking)**

Mozilla Firefox before 2.0.0.5 allows remote attackers to execute arbitrary code with

chrome privileges by calling an event handler from an unspecified "element outside of a document."

The issue has been fixed in Firefox 2.0.0.5.

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

References:

* BUGTRAQ: 20070720 rPSA-2007-0148-1 firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/474226/100/0/threaded
* BUGTRAQ: 20070724 FLEA-2007-0033-1: firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/474542/100/0/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-21.html
* CONFIRM:
ftp://ftp.slackware.com/pub/slackware/slackware-12.0/ChangeLog.txt
* CONFIRM:
http://support.novell.com/techcenter/psdb/07d098f99c9fe6956523beae37f32fda.html

CVE Reference: CVE-2007-3737

❖ **16621 Mozilla Firefox - Cross-domain handling exploited to inject arbitrary HTML and script code (Remote File Checking)**

Mozilla Firefox before 2.0.0.5 does not prevent use of document.write to replace an IFRAME during the load stage or in the case of an about:blank frame, which allows remote attackers to display arbitrary HTML or execute certain JavaScript code, as demonstrated by code that intercepts keystroke values from window.event, aka the "promiscuous IFRAME access bug,".

The issue has been fixed in Firefox 2.0.0.5.

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

References:

* BUGTRAQ: 20070604 Assorted browser vulnerabilities
http://www.securityfocus.com/archive/1/archive/1/470446/100/0/threaded
* BUGTRAQ: 20070720 rPSA-2007-0148-1 firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/474226/100/0/threaded
* BUGTRAQ: 20070724 FLEA-2007-0033-1: firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/474542/100/0/threaded
* FULLDISC: 20070604 Assorted browser vulnerabilities
http://archives.neohapsis.com/archives/fulldisclosure/2007-06/0026.html
* MISC:
http://lcamtuf.coredump.cx/ifsnatch/
* MISC:
https://bugzilla.mozilla.org/show_bug.cgi?id=381300

* MISC:
https://bugzilla.mozilla.org/show_bug.cgi?id=382686
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-20.html
* CONFIRM:
ftp://ftp.slackware.com/pub/slackware/slackware-12.0/ChangeLog.txt
* CONFIRM:
http://support.novell.com/techcenter/psdb/07d098f99c9fe6956523beae37f32fda.html

CVE Reference: CVE-2007-3089

❖ 16620 Mozilla Firefox - Arbitrary script injection into another site's context via timing issue (Remote File Checking)

Cross-site scripting (XSS) vulnerability in Mozilla Firefox before 2.0.0.5 allows remote attackers to inject arbitrary web script "into another site's context" via a "timing issue" involving the addEventListener or setTimeout functions, probably by setting events that activate after the context has changed.

The issue has been fixed in Firefox 2.0.0.5.

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

References:

* BUGTRAQ: 20070720 rPSA-2007-0148-1 firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/474226/100/0/threaded
* BUGTRAQ: 20070724 FLEA-2007-0033-1: firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/474542/100/0/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-19.html
* CONFIRM:
ftp://ftp.slackware.com/pub/slackware/slackware-12.0/ChangeLog.txt
* CONFIRM:
http://support.novell.com/techcenter/psdb/07d098f99c9fe6956523beae37f32fda.html

CVE Reference: CVE-2007-3736

❖ 16619 Mozilla Firefox - Javascript engine memory corruption, arbitrary code execution and denial of service Vulnerabilities (Remote File Checking)

Multiple unspecified vulnerabilities in the JavaScript engine in Mozilla Firefox before 2.0.0.5 and Thunderbird before 2.0.0.5 allow remote attackers to cause a denial of service (crash) via unspecified vectors that trigger memory corruption.

The issue has been fixed in Firefox 2.0.0.5.

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

References:

* BUGTRAQ: 20070720 rPSA-2007-0148-1 firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/474226/100/0/threaded
* BUGTRAQ: 20070724 FLEA-2007-0033-1: firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/474542/100/0/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-18.html
* CONFIRM:
ftp://ftp.slackware.com/pub/slackware/slackware-12.0/ChangeLog.txt
* CONFIRM:
http://support.novell.com/techcenter/psdb/07d098f99c9fe6956523beae37f32fda.html

CVE Reference: CVE-2007-3735

❖ 16618 Mozilla Firefox - Memory corruption, arbitrary code execution and denial of service Vulnerabilities (Remote File Checking)

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 2.0.0.5 and Thunderbird before 2.0.0.5 allow remote attackers to cause a denial of service (crash) via unspecified vectors that trigger memory corruption.

The issue has been fixed in Firefox 2.0.0.5.

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

References:

* BUGTRAQ: 20070720 rPSA-2007-0148-1 firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/474226/100/0/threaded
* BUGTRAQ: 20070724 FLEA-2007-0033-1: firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/474542/100/0/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-18.html
* CONFIRM:
ftp://ftp.slackware.com/pub/slackware/slackware-12.0/ChangeLog.txt
* CONFIRM:
http://support.novell.com/techcenter/psdb/07d098f99c9fe6956523beae37f32fda.html

CVE Reference: CVE-2007-3734

❖ 14056 Samba "winbind nss info" Privilege Escalation Security Issue

A security issue has been reported in Samba, which can be exploited by malicious, local users to gain escalated privileges.

The security issue is caused due to Winbind incorrectly assigning a primary group id of 0 to the queried domain user when "winbind nss info" is set to "sfu" or "rfc2307". This can

be exploited to gain escalated privileges, but requires that the RFC2307 or SFU (Services for Unix) primary group attributes are missing.

The security issue is reported in Samba versions from 3.0.25 to 3.0.25c.

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

References:

* SECUNIA: 26764
http://secunia.com/advisories/26764/
* MISC: CVE-2007-4138: Incorrect primary group assignment domain users using the rfc2307 or sfu winbind nss info plugin
http://us1.samba.org/samba/security/CVE-2007-4138.html
* BID: 25636
http://www.securityfocus.com/bid/25636/
* SECTRACK: 1018681
http://www.securitytracker.com/alerts/2007/Sep/1018681.html
* FRSIRT: FrSIRT/ADV-2007-3120
http://www.frsirt.com/english/advisories/2007/3120
* XF: 36560
http://xforce.iss.net/xforce/xfdb/36560

CVE Reference: CVE-2007-4138

❖ 16616 Windows Services for UNIX Could Allow Elevation of Privilege (MS07-053/939778) (Remote File Checking)

A vulnerability exists in Windows Services for UNIX 3.0, Windows Services for UNIX 3.5, and Subsystem for UNIX-based Applications where running certain setuid binary files could allow an attacker to gain elevation of privilege. An attacker who successfully exploited this vulnerability could gain elevation of privilege.

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

References:

* MS: MS07-053
http://www.microsoft.com/technet/security/Bulletin/MS07-053.mspx
* FRSIRT: ADV-2007-3115
http://www.frsirt.com/english/advisories/2007/3115
* SECUNIA: 26757
http://secunia.com/advisories/26757

CVE Reference: CVE-2007-3036

❖ 16615 Crystal Reports RPT Processing Vulnerability (MS07-052/941522) (Remote File Checking)

A remote code execution vulnerability exists in the way Crystal Reports for Visual Studio handles malformed RPT files. An attacker could exploit the vulnerability by sending an affected user a malformed RPT file as an e-mail attachment, or hosting the

file on a malicious or compromised Web site.

An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* BUGTRAQ: 20061123 LS-20061102 - Business Objects Crystal Reports Stack Overflow Vulnerability
http://www.securityfocus.com/archive/1/archive/1/452464/100/0/threaded
* MISC:
http://www.lssec.com/advisories/LS-20061102.pdf
* MS: MS07-052
http://www.microsoft.com/technet/security/Bulletin/MS07-052.mspx
* BID: 21261
http://www.securityfocus.com/bid/21261
* FRSIRT: ADV-2006-4691
http://www.frsirt.com/english/advisories/2006/4691
* FRSIRT: ADV-2007-3114
http://www.frsirt.com/english/advisories/2007/3114
* SECTRACK: 1017279
http://securitytracker.com/id?1017279
* SECUNIA: 23091
http://secunia.com/advisories/23091
* SECUNIA: 26754
http://secunia.com/advisories/26754
* XF: crystalreports-rpt-bo(30532)
http://xforce.iss.net/xforce/xfdb/30532

CVE Reference: CVE-2006-6133

❖ 16614 Microsoft Agent Remote Code Execution Vulnerability (MS07-051/938827) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Agent in the way that it handles certain specially crafted URLs. The vulnerability could allow an attacker to remotely execute code on the affected system. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* BUGTRAQ: 20070911 Assurent VR - Microsoft Agent Crafted URL Stack Buffer Overflow
http://www.securityfocus.com/archive/1/archive/1/479096/100/0/threaded
* MS: MS07-051
http://www.microsoft.com/technet/security/Bulletin/MS07-051.mspx

* FRSIRT: ADV-2007-3113
http://www.frsirt.com/english/advisories/2007/3113
* SECUNIA: 26753
http://secunia.com/advisories/26753

CVE Reference: CVE-2007-3040

New Vulnerabilities found this Week

Cisco IOS Regular Expressions Denial of Service
"Denial of Service"

A vulnerability has been reported in Cisco IOS, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error when handling regular expressions containing repetition operators and pattern recalls. This can be exploited to cause a stack overflow by sending a command with specially crafted regular expressions to the command line interface.

Successful exploitation causes the device to crash and requires a reboot, but requires valid user credentials.

The vulnerability is reported in versions 12.0, 12.1, 12.2, 12.3, and 12.4.

References:
http://www.cisco.com/en/US/products/products_security_response09186a00808bb91c.html
https://puck.nether.net/pipermail/cisco-nsp/2007-August/043002.html

Media Player Classic AVI File Processing Buffer Overflow
"Execution of arbitrary code"

Code Audit Labs has discovered a vulnerability in Media Player Classic, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an input validation error when processing .AVI files and can be exploited to cause a buffer overflow via a .AVI file with a specially crafted "indx" chunk.

Successful exploitation allows execution of arbitrary code.

The vulnerability is confirmed in version 6.4.9.0. Other versions may also be affected.

References:
http://www.vulnhunt.com/advisories/CAL-20070912-1_Multiple_vendor_produce_handling_AVI_file_vulnerabilities.txt

Microsoft Windows Services for UNIX Privilege Escalation

"Gain escalated privileges"

A vulnerability has been reported in Microsoft Windows Services for UNIX, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to an unspecified error in Windows Services for UNIX and the Subsystem for UNIX-based Applications component when handling connection credentials for setuid binaries. This can be exploited to execute arbitrary code with escalated privileges by running a specially crafted setuid binary.

Successful exploitation requires that Windows Services for UNIX is installed or the Subsystem for UNIX-based Applications component is enabled (disabled by default).

NOTE: According to Microsoft, "limited distribution" of the vulnerability details already exists.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-053.mspx
http://descriptions.securescout.com/tc/16616

Samba "winbind nss info" Privilege Escalation Security Issue

"Gain escalated privileges"

A security issue has been reported in Samba, which can be exploited by malicious, local users to gain escalated privileges.

The security issue is caused due to Winbind incorrectly assigning a primary group id of 0 to the queried domain user when "winbind nss info" is set to "sfu" or "rfc2307". This can be exploited to gain escalated privileges, but requires that the RFC2307 or SFU (Services for Unix) primary group attributes are missing.

The security issue is reported in Samba versions from 3.0.25 to 3.0.25c.

References:
http://samba.org/samba/security/CVE-2007-4138.html
http://descriptions.securescout.com/tc/14056

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