netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 39

September 29, 2006

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).

This Week in Review

Software flaws a possible money-maker for the very same companies. Professionals in the industry fear new computer crime laws. Mobile data security a growing issue. Gap between how important developers and managers rate security.

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

- **Should Microsoft be in the anti-malware business?**

Microsoft has a cadre of anti-malware tools. Most are free, but some current and forthcoming options are commercial. Any marketplace entry by the Redmond-based company becomes an immediate formidable foe lessening competitor profits.
Many analysts are asking if Microsoft, which could be blamed for creating the very insecurities that Windows malware is exploiting, should be able to reap additional profit from closing those same holes? The company's worst critics are worried that key

vulnerabilities could be left in Windows longer to benefit additional Microsoft revenue streams.
I think it is a fair question, and I encourage the discussion and debate. I admit to having mixed emotions, but I ultimately support Microsoft's objectives as long as they compete in the anti-malware marketplace fairly. Here's why.

InfoWorld

Full Story :
http://www.infoworld.com/article/06/09/29/40OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/06/09/29/40OPsecadvise_1.html

❖ Security professionals at risk from hacking laws

Company networks could be made less secure if projected computer crime legislation is introduced in several European countries. According to several security professionals, that would be the unintended consequence of anti-hacking laws.
The UK and Germany are among the countries that are considering revisions to their computer crime laws in line with the 2001 Convention on Cybercrime, a Europe-wide treaty, and with a similar European Union measure passed in early 2005.

But security professionals are scrutinising those revisions out of concern for how prosecutors and judges could apply the laws. Security professionals are especially concerned about cases where the revisions apply to programs that could be used for bad or good. Companies often use hacking programs to test the mettle of their own systems.

TechWorld

Full Story :
http://www.techworld.com/security/news/index.cfm?newsID=6990&pagtype=samechan

❖ Managing Mobile Data Security

"Information leakage", as it is sometimes termed, is a growing issue for corporations with the increasing availability and decreasing cost of high density flash memory. Flash is present in nearly every consumer gadget, but of particular concern to network administrators are personal productivity tools like USB memory sticks, smart phones, PDAs, and of course mobile email devices.

Mobile email represents yet another security headache for administrators, a fait accompli due to its popularity with senior management, with encrypted attachments crossing the firewall, making inspection difficult or impossible. Once the data is on the mobile device it can be easily compromised through loss or theft. Since mobile email devices have been adopted top-down in organizations, the lost data is likely to be very sensitive, raising major questions of compliance and protection of intellectual property. You can pretty much guarantee that senior executives email drafts of quarterly earnings reports between each other.

IT Analysis

Full Story :
http://www.it-analysis.com/business/content.php?cid=8814

- **Survey Shows Gap Between Developers, Corporate Security Priorities**

A recent survey of 400 U.S.-based application developers and programmers showed that while those who build Web applications are more concerned about security than ever before, corporate resources and processes that increase application security aren't as forthcoming.

According to the survey released last week, which was conducted in June by Applied Research and sponsored by security vendor Symantec, 93 percent of the developers and programmers who responded said that secure application development is a higher priority than it was three years ago, with 35 percent ranking it as their No. 1 priority.

-- advertisement --

But while those building the applications seem to get the need for security, those employing them don't seem to have caught on quite as strongly. For example, of those surveyed, only 65 percent say that security is part of their company's QA process, and only 12 percent report that security is always a priority over meeting deadlines.

Mcp Magazine

Full Story :
http://www.mcpmag.com/news/article.asp?EditorialsID=1053

New Vulnerabilities Tested in SecureScout

- **12138 OpenSSL error in the processing of certain invalid ASN.1 structures leading to system resources consumption Vulnerability**

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

An error in the processing of certain invalid ASN.1 structures can be exploited to cause an infinite loop and consume system memory in an application using OpenSSL to process ASN.1 data from untrusted sources.

NOTE: This does not affect versions prior to 0.9.7.

The vulnerability is reported in versions 0.9.7k and 0.9.8c. Prior versions may also be affected.

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

References:

Original advisory:
http://www.openssl.org/news/secadv_20060928.txt

Other references:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2937
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2940
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3738
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4343

CVE Reference: CVE-2006-2937

❖ 12139 OpenSSL overly long time taken to process certain types of public keys leading to Denail of Service Vulnerability

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

Certain types of public keys take overly long time to process and can be exploited to cause a DoS in an application using OpenSSL to process ASN.1 data from untrusted sources.

The vulnerability is reported in versions 0.9.7k and 0.9.8c. Prior versions may also be affected.

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

References:

Original advisory:
http://www.openssl.org/news/secadv_20060928.txt

Other references:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2937
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2940
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3738
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4343

CVE Reference: CVE-2006-2937

❖ 12140 OpenSSL error in the "SSL_get_shared_ciphers()" function, code execution Vulnerability

A vulnerability has been reported in OpenSSL, which can be exploited by malicious people to execute code.

An error in the "SSL_get_shared_ciphers()" function can be exploited to cause a buffer overflow by sending a list of ciphers to an application using the vulnerable function.

The vulnerability is reported in versions 0.9.7k and 0.9.8c. Prior versions may also be affected.

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

References:

Original advisory:
http://www.openssl.org/news/secadv_20060928.txt

Other references:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2937
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2940
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3738
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4343

CVE Reference: CVE-2006-2937

❖ 12141 OpenSSL error in the SSLv2 client code to crash a vulnerable client Vulnerability

A vulnerability has been reported in OpenSSL, which can be exploited by malicious people to crash client program.

An error in the SSLv2 client code can be exploited by a malicious server to crash a vulnerable client using OpenSSL to create an SSLv2 connection to the server.

The vulnerability is reported in versions 0.9.7k and 0.9.8c. Prior versions may also be affected.

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

References:

Original advisory:
http://www.openssl.org/news/secadv_20060928.txt

Other references:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2937
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2940
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3738
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4343

CVE Reference: CVE-2006-2937

❖ 16340 Vulnerability in PowerPoint Could Allow Remote Code Execution (925984) (Remote File Checking)

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

The vulnerability is due to an unspecified error when processing PowerPoint documents containing a malformed string. This can be exploited to corrupt system memory and may allow execution of arbitrary code when a malicious PowerPoint

document is opened.

NOTE: This vulnerability is reportedly being exploited in the wild.

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

References:

Original advisory:
http://www.microsoft.com/technet/security/advisory/925984.mspx

Other references:
MISC: http://www.avertlabs.com/research/blog/?p=95
MISC: http://vil.nai.com/vil/content/v_140666.htm
CERT-VN:VU#231204
URL:http://www.kb.cert.org/vuls/id/231204
BID:20226
URL:http://www.securityfocus.com/bid/20226
FRSIRT:ADV-2006-3794
URL:http://www.frsirt.com/english/advisories/2006/3794

CVE Reference: CVE-2006-4694

❖ 16341 Microsoft Internet Explorer "WebViewFolderIcon" Integer Overflow (Remote File Checking)

H D Moore has discovered a vulnerability in Microsoft Internet Explorer, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an integer overflow error in the "setSlice()" method in the "WebViewFolderIcon" ActiveX control. This can be exploited to corrupt memory when e.g. visiting a malicious web site.

Successful exploitation allows execution of arbitrary code.

NOTE: Exploit code is publicly available.

The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2. Other versions may also be affected.

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

References:

Original advisory:
http://browserfun.blogspot.com/2006/07/mobb-18-webviewfoldericon-setslice.html

Other references:
BUGTRAQ:20060927 Exploit module available for WebViewFolderIcon setSlice 0-day
URL:http://www.securityfocus.com/archive/1/archive/1/447174/100/0/threaded

MISC: http://riosec.com/msie-setslice-vuln
CERT:TA06-270A
URL:http://www.us-cert.gov/cas/techalerts/TA06-270A.html
CERT-VN:VU#753044
URL:http://www.kb.cert.org/vuls/id/753044
BID:19030
URL:http://www.securityfocus.com/bid/19030
OSVDB:27110
URL:http://www.osvdb.org/27110
XF:ie-webviewfoldericon-dos(27804)
URL:http://xforce.iss.net/xforce/xfdb/27804

CVE Reference: CVE-2006-3730

❖ 16342 Linux Kernel ELF Cross-Region Mapping Denial of Service Vulnerability

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

The vulnerability is caused due to an error on IA64 and SPARC platforms when handling certain ELF files. This can be exploited to crash the system via a specially crafted ELF file.

The vulnerability has been reported in versions 2.6.17.10 and bellow.

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

References:

Original advisory:
http://lkml.org/lkml/2006/9/4/116
http://www.kernel.org/git/?p=linux/kernel/git/stable/linux-2.6.17.y.git;a=commit;h=8833ebaa3f4325820fe3338ccf6fae04f6669254
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.17.11

Other references:
UBUNTU:USN-347-1
URL:http://www.ubuntu.com/usn/usn-347-1
BID:19702
URL:http://www.securityfocus.com/bid/19702
FRSIRT:ADV-2006-3670
URL:http://www.frsirt.com/english/advisories/2006/3670
SECUNIA:21999
URL:http://secunia.com/advisories/21999

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-4538

❖ 16343 Linux Kernel ULE Packet Handling Denial of Service Vulnerability

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

The vulnerability is caused due to an error in the ULE (Unidirectional Lightweight Encapsulation) decapsulation code when processing ULE packets. This can be exploited to crash the system by sending a malicious ULE packet with an SNDU (Sub Network Data Unit) size of 0.

The vulnerability has been reported in version 2.6.17.11. Other versions may also be affected.

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

References:

Original advisory:
MLIST:[lkml-patch] 20060821 dvb-core: Proper handling ULE SNDU length of 0
http://lkml.org/lkml/2006/8/20/278

Other references:
BID:19939
URL:http://www.securityfocus.com/bid/19939
FRSIRT:ADV-2006-3551
URL:http://www.frsirt.com/english/advisories/2006/3551
SECUNIA:21820
URL:http://secunia.com/advisories/21820

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-4623

❖ 16344 Linux Kernel error in the "elv_unregister()" function, Crash Vulnerability

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

An error in the "elv_unregister()" function on module unload may cause a crash by an exiting task or process.

The vulnerability has been reported in version 2.6.17.9. Other versions may also be affected.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.17.10

Other references:
http://lkml.org/lkml/2006/6/16/6

Product Homepage:
http://kernel.org/

CVE Reference:

- **16345 Linux Kernel error in the "sctp_make_abort_user()" function leading to execution of arbitrary code with escalated privileges Vulnerability**

A vulnerability has been reported in the Linux Kernel, which can be exploited by malicious, local users to gain escalated privileges.

An error in the SCTP module within the "sctp_make_abort_user()" function can be exploited to execute arbitrary code with escalated privileges.

The vulnerability has been reported in version 2.6.17.9. Other versions may also be affected.

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

References:

Original advisory:
BUGTRAQ:20060822 Linux Kernel SCTP Privilege Elevation Vulnerability
http://www.securityfocus.com/archive/1/archive/1/444066/100/0/threaded

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-3745

New Vulnerabilities found this Week

Microsoft PowerPoint Code Execution Vulnerability

"Corrupt system memory; execution of arbitrary code"

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

The vulnerability is due to an unspecified error when processing PowerPoint documents containing a malformed string. This can be exploited to corrupt system memory and may allow execution of arbitrary code when a malicious PowerPoint document is opened.

NOTE: This vulnerability is reportedly being exploited in the wild.

References:
http://www.microsoft.com/technet/security/advisory/925984.mspx
http://www.kb.cert.org/vuls/id/231204
http://descriptions.securescout.com/tc/16340

Microsoft Internet Explorer "WebViewFolderIcon" Integer Overflow

"Execution of arbitrary code"

H D Moore has discovered a vulnerability in Microsoft Internet Explorer, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an integer overflow error in the "setSlice()" method in the "WebViewFolderIcon" ActiveX control. This can be exploited to corrupt memory when e.g. visiting a malicious web site.

Successful exploitation allows execution of arbitrary code.

NOTE: Exploit code is publicly available.

The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2. Other versions may also be affected.

References:
http://browserfun.blogspot.com/2006/07/mobb-18-webviewfoldericon-setslice.html
http://descriptions.securescout.com/tc/16341

Microsoft Vector Graphics Rendering Library Buffer Overflow

"Execution of arbitrary code"

A vulnerability has been discovered in Microsoft Windows, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the Microsoft Vector Graphics Rendering(VML) library (vgx.dll) when processing certain content in Vector Markup Language (VML) documents. This can be exploited to cause a stack-based buffer overflow by e.g. tricking a user into viewing a malicious VML document containing an overly long "fill" method inside a "rect" tag with the Internet Explorer browser.

Successful exploitation allows execution of arbitrary code with the privileges of the application using the vulnerable functionality in the library.

NOTE: The vulnerability is currently being actively exploited.

The vulnerability is confirmed on a fully patched Microsoft Windows XP SP2 system. Other versions may also be affected.

According to Microsoft, other unspecified vulnerabilities also exist.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-055.mspx
http://www.microsoft.com/technet/security/advisory/925568.mspx
http://descriptions.securescout.com/tc/16337

OpenSSL Multiple Denial of Service Vulnerabilities

"Denial of Service"

Some vulnerabilities have been reported in OpenSSL, which can be exploited by malicious people to cause a DoS (Denial of Service).

1) An error in the processing of certain invalid ASN.1 structures can be exploited to cause an infinite loop and consume system memory in an application using OpenSSL to process ASN.1 data from untrusted sources.

NOTE: This does not affect versions prior to 0.9.7.

2) Certain types of public keys take overly long time to process and can be exploited to cause a DoS in an application using OpenSSL to process ASN.1 data from untrusted sources.

3) An error in the "SSL_get_shared_ciphers()" function can be exploited to cause a buffer overflow by sending a list of ciphers to an application using the vulnerable function.

4) An error in the SSLv2 client code can be exploited by a malicious server to crash a vulnerable client using OpenSSL to create an SSLv2 connection to the server.

References:
http://www.openssl.org/news/secadv_20060928.txt
http://descriptions.securescout.com/tc/12138
http://descriptions.securescout.com/tc/12139
http://descriptions.securescout.com/tc/12140
http://descriptions.securescout.com/tc/12141

OpenSSH Identical Blocks Denial of Service Vulnerability

"Denial of Service"

Tavis Ormandy has reported a vulnerability in OpenSSH, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the handling of multiple identical blocks in a ssh packet. If ssh protocol 1 is enabled, this can be exploited to cause a DoS due to CPU consumption by sending specially crafted ssh packets.

References:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=207955

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