netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 36

September 8, 2006

Table of Contents

Product Focus

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

This Week in Review

Five Major credit card companies teaming up. Phishing on the rise and narrowing targets. Profit the key for malware authors. Enigma code braker box rebuilt.

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

- **Credit card companies team up for security**

The five major credit card companies have teamed up in the interest of better security.

American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International announced Thursday the creation of an organisation to develop and maintain security standards for credit and debit card payments. It's the first time the five brands have agreed on a single, common framework.
The newly formed Payment Card International (PCI) Security Standards Council will

manage the PCI Data Security Standard, first established in January 2005 with the intention of making its implementation more efficient for all parties involved in a payment card transaction. That includes merchants, payment processors, point-of-sale vendors, financial institutions and more than a billion card holders worldwide.

ZDNet

Full Story :
http://news.zdnet.co.uk/business/0,39020645,39282935,00.htm

❖ Phishers cast nets less wide

More scams hitting fewer targets, says report.

According to RSA Security's August report on online fraud, the number of brands attacked by phishing scams fell by 20% last month, despite an overall rise in the level of phishing attempts seen.

The number of targets outside the US rose slightly, but US-based companies are still by far the most frequently hit by phishers, with 73% of all targets based there. Credit unions and regional banks take the lion's share, with national banks targeted by less than 20% of phishes.

The US is also the top source of attacks, although the share fell to less than 50% for the first time in a while. Four other countries, Germany, Australia, Estonia (a relative newcomer) and Sweden, make up almost 40% of phish sources between them, while China - previously a major source - fell outside the top ten.

virusbulletin

Full Story :
http://www.virusbtn.com/news/spam_news/2006/09_08.xml?rss=

❖ Malware authors hungry for profit

The vast majority of malware is created with criminal intent as black-hat hackers turn from technical one-upmanship to seeking real financial gain, according to a new report.

Some 88 per cent of the new malware detected in the second quarter of 2006 was related to cyber-crime, reported PandaLabs in its latest global report.

"The results show how malware creators are concentrating on profiting from their efforts, creating increasing numbers of Trojans and bots," said Luis Corrons, director of PandaLabs.

"The greatest danger is that Trojans are installed and operate silently without users noticing any of the typical symptoms of infection, and victims are unaware that their computers are being used to steal from them or even from third parties."

vunet

Full Story :

http://www.vnunet.com/vnunet/news/2163699/malware-profit

- **The box that broke Enigma code is rebuilt**

Turing Bombe replica goes on show

Enthusiasts have succeeded in rebuiling a Nazi code cracking device, signaling the culmination of a 10-year project.

The replica Turing Bombe, a recreation of an electromagnetic machine used by British codebreakers to help decipher Nazi codes used during World War Two, was unveiled on Wednesday at Bletchley Park, the centre of British code-breaking efforts during the war.

Bombes automated the process of cracking the Nazi's Enigma code. Enigma devices had three rotors, each with 26 possible positions, creating 17,576 possible combinations for each letter. The devices tried every possible rotor position and applied test to weed out a much smaller number of possible solutions, which were then checked by hand. The whole process relied on using a small section of ciphertext, to which cryptographers had guessed corresponding plain text in order to extract the likely settings used to produce a much longer message.

The Register

Full Story :
http://www.theregister.co.uk/2006/09/08/turing_bombe_rebuild/

New Vulnerabilities Tested in SecureScout

- **12135 OpenSSL RSA Signature Forgery Vulnerability**

A vulnerability has been reported in OpenSSL, which potentially can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to an error within the verification of certain signatures. If an RSA key with exponent 3 is used, it may be possible to forge a PKCS #1 v1.5 signature signed by that key.

The vulnerability is reported in versions 0.9.7j and 0.9.8b. 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_20060905.txt

Other references:
MLIST:[ietf-openpgp] 20060827 Bleichenbacher's RSA signature forgery based on implementation error
URL:http://www.imc.org/ietf-openpgp/mail-archive/msg14307.html
CONFIRM: http://www.openssl.org/news/secadv_20060905.txt

BID:19849
URL:http://www.securityfocus.com/bid/19849
FRSIRT:ADV-2006-3453
URL:http://www.frsirt.com/english/advisories/2006/3453
SECUNIA:21709
URL:http://secunia.com/advisories/21709
UBUNTU:USN-339-1
URL:http://www.ubuntu.com/usn/usn-339-1

CVE Reference: CVE-2006-4339

❖ 12136 OpenSSL Potential SSL 2.0 Rollback Vulnerability

A vulnerability has been reported in OpenSSL, which potentially can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to an error in handling the use of SSL_OP_MSIE_SSLV2_RSA_PADDING option. The use of this option causes a verification check that prevents protocol-version rollback attacks to be disabled. This may be exploited in "man-in-the-middle" attacks to force a client and a server to negotiate the less secure SSL 2.0 protocol even when both parties support the more secure SSL 3.0 or TLS 1.0 protocols. The option is also enabled when the SSL_OP_ALL option is used.

Successful exploitation requires that SSL 2.0 is enabled, and either the SSL_OP_MSIE_SSLV2_RSA_PADDING or the SSL_OP_ALL option is used.

The vulnerability has been reported in all versions prior to 0.9.7h, and prior to 0.9.8a.

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

References:

Original advisory:
http://www.openssl.org/news/secadv_20060905.txt

CVE Reference: CVE-2005-2969

❖ 16319 Vulnerability in Word Could Allow Remote Code Execution (925059) (Remote File Checking)

A vulnerability has been discovered in Microsoft Word 2000, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a memory corruption error in WINWORD.EXE when processing Word documents. This can be exploited to execute arbitrary code when a malicious document is opened.

The vulnerability is being actively exploited.

The vulnerability is confirmed in a fully patched Microsoft Word 2000 and has currently not been confirmed in other versions. However, they may be affected.

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

References:

Original advisory:
http://www.microsoft.com/technet/security/advisory/925059.mspx

Other References:
* US-CERT VU#806548:
http://www.kb.cert.org/vuls/id/806548
* MISC: http://blogs.securiteam.com/?p=586
* MISC: http://isc.sans.org/diary.php?storyid=1669
* MISC:
http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-090219-2855-99
* MISC: http://vil.mcafeesecurity.com/vil/content/v_119055.htm
* CONFIRM: http://www.microsoft.com/technet/security/advisory/925059.mspx
* BID:19835
* URL:http://www.securityfocus.com/bid/19835
* FRSIRT:ADV-2006-3448
* URL:http://www.frsirt.com/english/advisories/2006/3448
* SECTRACK:1016787
* URL:http://securitytracker.com/id?1016787
* SECUNIA:21735
* URL:http://secunia.com/advisories/21735

CVE Reference: CVE-2006-4534

❖ 16320 IMail IMAP Service LIST command Denial of Service Vulnerability

A vulnerability has been reported in IMail Server, which can be exploited to cause a DoS (Denial of Service).

An error exists in the IMAP4D32 service when handling user supplied arguments passed to the IMAP LIST command. This can be exploited by a logon user to cause a memory dereferencing error, which crashes the IMAP service by supplying an argument of approximately 8000 bytes to the command.

The vulnerabilities have been reported in IMail Server version 8.20. Other versions prior to 8.22 may also be affected.

IMail Server is included as part of the Ipswitch Collaboration Suite.

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

References:

Initial Advisory :
* IDEFENSE:20051206 Ipswitch IMail IMAP List Command DoS Vulnerability

* URL:http://www.idefense.com/application/poi/display?id=347&type=vulnerabilities

Other references:
* BID:15753
* URL:http://www.securityfocus.com/bid/15753
* FRSIRT:ADV-2005-2782
* URL:http://www.frsirt.com/english/advisories/2005/2782
* SECTRACK:1015318
* URL:http://securitytracker.com/id?1015318
* SECUNIA:17863
* URL:http://secunia.com/advisories/17863

Product HomePage:
http://www.ipswitch.com/Products/IMail_Server/index.html

CVE Reference: CVE-2005-2923

❖ 16321 IMail IMAP Service FETCH command Denial of Service Vulnerability

FistFuXXer has reported a vulnerability in Ipswitch IMail Server/Collaboration Suite, which can be exploited by malicious users to cause a DoS (Denial of Service) and potentially to compromise a vulnerable system.

The vulnerability is caused due to a boundary error within the handling of the IMAP FETCH command. This can be exploited to cause a buffer overflow, which crashes the server and allows arbitrary code execution via an overly long argument.

The vulnerability has been reported in the following versions:
* Ipswitch Collaboration Suite 2006 Premium Edition
* Ipswitch Collaboration Suite 2006 Standard Edition
* IMail Secure Server 2006
* IMail Server 2006

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

References:

Initial Advisory :
MISC: http://www.zerodayinitiative.com/advisories/ZDI-06-003.html

Other references:
BUGTRAQ:20060313 ZDI-06-003: Ipswitch Collaboration Suite Code Execution Vulnerability
URL:http://www.securityfocus.com/archive/1/archive/1/427536/100/0/threaded
CONFIRM: http://www.ipswitch.com/support/ics/updates/ics200603prem.asp
BID:17063
URL:http://www.securityfocus.com/bid/17063
FRSIRT:ADV-2006-0907
URL:http://www.frsirt.com/english/advisories/2006/0907
OSVDB:23796
URL:http://www.osvdb.org/23796

SECTRACK:1015759
URL:http://securitytracker.com/id?1015759
SECUNIA:19168
URL:http://secunia.com/advisories/19168
XF:ipswitch-imap-fetch-bo(25133)
URL:http://xforce.iss.net/xforce/xfdb/25133

Product HomePage:
http://www.ipswitch.com/Products/IMail_Server/index.html

CVE Reference: CVE-2005-3526

❖ 16322 IMail SMTP Service Code Execution Vulnerability

A vulnerability has been reported in IMail Server, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an unspecified error in the SMTP daemon and can be exploited to execute arbitrary code.

The vulnerability is reported in the following versions:
* Ipswitch Collaboration 2006 Suite Premium Edition
* Ipswitch Collaboration 2006 Suite Standard Edition
* IMail
* IMail Plus
* IMail Secure

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

References:

Initial Advisory :
http://www.ipswitch.com/support/imail/releases/im20061.asp
http://www.ipswitch.com/support/ics/updates/ics20061.asp

Other references:
http://www.securityfocus.com/bid/19885/references
http://secunia.com/advisories/21795/

Product HomePage:
http://www.ipswitch.com/Products/IMail_Server/index.html

CVE Reference:

❖ 16323 BIND Zone Transfer TSIG Handling Denial of Service Vulnerability

A vulnerability been reported in ISC BIND, 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 the TSIG in the

second or subsequent messages in a zone transfer. This can be exploited to crash "named" via a malformed TSIG in the messages.

Successful exploitation requires that the first zone transfer message have a valid TSIG.

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

References:

Original advisory:
http://www.niscc.gov.uk/niscc/docs/re-20060425-00312.pdf?lang=en

Other references:
MISC: http://www.niscc.gov.uk/niscc/docs/re-20060425-00312.pdf?lang=en
MISC: http://www.niscc.gov.uk/niscc/docs/br-20060425-00311.html?lang=en
CERT-VN:VU#955777
URL:http://www.kb.cert.org/vuls/id/955777
BID:17692
URL:http://www.securityfocus.com/bid/17692
FRSIRT:ADV-2006-1505
URL:http://www.frsirt.com/english/advisories/2006/1505
FRSIRT:ADV-2006-1537
URL:http://www.frsirt.com/english/advisories/2006/1537
SECUNIA:19808
URL:http://secunia.com/advisories/19808
SECTRACK:1015993
URL:http://securitytracker.com/id?1015993

Product Homepage:
http://www.isc.org/

CVE Reference: CVE-2006-2073

❖ 16324 BIND SIG queries crash Vulnerability

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

An assertion error within the processing of SIG queries can be exploited to crash either a recursive server when more than one SIG(covered) Resource Record set (RRset) is returned or an authoritative server serving a RFC 2535 DNSSEC zone where there are multiple SIG(covered) RRsets.

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

References:

Original advisory:
http://www.isc.org/sw/bind/bind-security.php

Other references:
MISC: http://www.niscc.gov.uk/niscc/docs/re-20060905-00590.pdf?lang=en
CERT-VN:VU#915404
URL:http://www.kb.cert.org/vuls/id/915404

FRSIRT:ADV-2006-3473
URL:http://www.frsirt.com/english/advisories/2006/3473
SECTRACK:1016794
URL:http://securitytracker.com/id?1016794
SECUNIA:21752
URL:http://secunia.com/advisories/21752

Product Homepage:
http://www.isc.org/

CVE Reference: CVE-2006-4095

❖ 16325 BIND INSIST failure Denial of service Vulnerability

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

An error within the handling of multiple recursive queries can be exploited to trigger an INSIST failure by causing the response to the query to arrive after all clients looking for the response have left the recursion queue.

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

References:

Original advisory:
http://www.isc.org/sw/bind/bind-security.php

Other references:
MISC: http://www.niscc.gov.uk/niscc/docs/re-20060905-00590.pdf?lang=en
CERT-VN:VU#697164
URL:http://www.kb.cert.org/vuls/id/697164
FRSIRT:ADV-2006-3473
URL:http://www.frsirt.com/english/advisories/2006/3473
SECTRACK:1016794
URL:http://securitytracker.com/id?1016794
SECUNIA:21752
URL:http://secunia.com/advisories/21752

Product Homepage:
http://www.isc.org/

CVE Reference: CVE-2006-4096

❖ 16326 Linux Kernel UDF Denial of Service 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).

The vulnerability is due to an error in UDF and can be exploited to cause the system to stop responding when truncating certain files.

The vulnerability has been reported in versions prior to 2.6.17.10 or 2.4.33.3.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.33.3
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.17.10

Other references:
MISC: http://lkml.org/lkml/2006/6/16/6
BID:19562
URL:http://www.securityfocus.com/bid/19562
FRSIRT:ADV-2006-3308
URL:http://www.frsirt.com/english/advisories/2006/3308
SECUNIA:21515
URL:http://secunia.com/advisories/21515

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-4145

New Vulnerabilities found this Week

Microsoft Word 2000 Unspecified Code Execution Vulnerability
"Execute arbitrary code"

A vulnerability has been discovered in Microsoft Word 2000, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a memory corruption error in WINWORD.EXE when processing Word documents. This can be exploited to execute arbitrary code when a malicious document is opened.

NOTE: The vulnerability is being actively exploited.

The vulnerability is confirmed in a fully patched Microsoft Word 2000 and has currently not been confirmed in other versions. However, they may be affected.

References:
http://www.microsoft.com/technet/security/advisory/925059.mspx
http://www.kb.cert.org/vuls/id/806548
http://descriptions.securescout.com/tc/16319

Ipswitch IMail Server SMTP Service Unspecified Vulnerability
"Execute arbitrary code"

A vulnerability has been reported in IMail Server, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an unspecified error in the SMTP daemon and can be exploited to execute arbitrary code.

The vulnerability is reported in the following versions:
* Ipswitch Collaboration 2006 Suite Premium Edition
* Ipswitch Collaboration 2006 Suite Standard Edition
* IMail
* IMail Plus
* IMail Secure

References:
http://www.ipswitch.com/support/ics/updates/ics20061.asp
http://www.ipswitch.com/support/imail/releases/im20061.asp
http://descriptions.securescout.com/tc/16322

ISC BIND Denial of Service Vulnerabilities
"Denial of Service"

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

1) An assertion error within the processing of SIG queries can be exploited to crash either a recursive server when more than one SIG(covered) Resource Record set (RRset) is returned or an authoritative server serving a RFC 2535 DNSSEC zone where there are multiple SIG(covered) RRsets.

2) An error within the handling of multiple recursive queries can be exploited to trigger an INSIST failure by causing the response to the query to arrive after all clients looking for the response have left the recursion queue.

NOTE: According to the vendor, the vulnerabilities are likely not exploitable in the 9.2.x branch. However, a patch has been provided.

References:
http://www.isc.org/sw/bind/bind-security.php
http://www.kb.cert.org/vuls/id/697164
http://www.kb.cert.org/vuls/id/915404
http://descriptions.securescout.com/tc/16324
http://descriptions.securescout.com/tc/16325

Cisco IOS GRE Decapsulation Vulnerability
"Bypass access control lists"

FX has reported a vulnerability in Cisco IOS, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to an error within the handling of GRE packets with source routing information as the offset field is not verified before being used to decapsulate a packet. This can potentially be exploited to bypass access control lists on the router by sending specially crafted packets.

The vulnerability affects Cisco IOS 12.0, 12.1, and 12.2 based trains when configured with

GRE IP or GRE IP multipoint tunnels.

NOTE: Cisco IOS version 12.0S, with a revision later than 12.0(23)S, with CEF enabled is not affected.

References:
http://www.phenoelit.de/stuff/CiscoGRE.txt
http://www.cisco.com/warp/public/707/cisco-sr-20060906-gre.shtml

OpenSSL RSA Signature Forgery Vulnerability

"Bypass certain security restrictions"

A vulnerability has been reported in OpenSSL, which potentially can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to an error within the verification of certain signatures. If an RSA key with exponent 3 is used, it may be possible to forge a PKCS #1 v1.5 signature signed by that key.

The vulnerability is reported in versions 0.9.7j and 0.9.8b. Prior versions may also be affected.

References:
http://www.openssl.org/news/secadv_20060905.txt
http://descriptions.securescout.com/tc/12135

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