netVigilance
assurance has arrived

2008 Issue # 11

ScoutNews

The weekly Security update from the makers of SecureScout

March 14, 2008

Table of Contents

Product Focus

This Week in Review

Top Security News Stories this Week

New Vulnerabilities Tested in SecureScout

New Vulnerabilities found this Week

Product Focus

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.

Jesper Jurcenoks of netVigilance is keynote speaker at ITEC's "Master Mind Panel and Lunch: Security for Second Circle Technologies", the first in Houston May 7-8, see **http://www.netvigilance.com/events**

This Week in Review

web 2.0 and security - once again. Some sound advice about how to act when using public wi-fi's. A new way to give secure access to your network. Backgrounder about internet and crime.

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

❖ Avoid data leakage in a Web 2.0 world

Losing data such as intellectual property can harm an organisation competitively and, if it can be proven how the loss occurred and what party benefited, can potentially lead to expensive litigation.

Businesses face many regulations that force them to improve their security and implement safeguards. In a recent Quocirca survey 82 per cent of 250 respondents cited data protection laws as the most worrying regulation they face - more than twice as many as for any other.

Computer active

Full Story :
http://www.computeractive.co.uk/crn/analysis/2211971/avoid-leakage-web-world-3877661

❖ Public Wi-Fi: Be Very Paranoid

Public Wi-Fi: Be Very Paranoid
Wireless services in airports, cafés, and hotels are often not encrypted. So user beware
You have an hour before your flight, so you log in to the Wi-Fi network at the airport. You look up some stock prices, check your e-mail, pay a couple of bills online, and surf a few Web sites. Has it occurred to you that curious or hostile eyes could be peering into your computer and your network? It pays to be paranoid.

The wireless service offered in airports, coffee shops, hotels, and other hotspots is almost always unencrypted. That means anyone else on the network who is equipped with readily available software can read your transmissions with little effort. And when there is protection, it's likely to be a form of encryption called Wired Equivalent Privacy (WEP) that's easily broken.

businessweek

Full Story :
http://www.businessweek.com/magazine/content/08_12/b4076000604104.htm?campaign_id=rss_daily

❖ Knock, Knock...Who's there? Port Knock!

Sprinkle a new layer of security on your network
In our society, it often takes tragedy, to bring about change; unfortunate, but true. I am no exception. Over the weekend, I may have accidentally left a few ports open. With 65,535 of them, it's hard to remember if they're all closed and stealthed, or if 1241 is still open from my Nessus session, if my Slingbox is still slinging shows over 5001, or if one of those ports in the 27000 range was left open by my alter-ego, half-life addict.

Lucky for me, someone kindly let me know that some ports were left open, through the generous installation of free software (trojans, key loggers, and other malware goodies) on my server and several PCs. After some digital house cleaning, I decided to sprinkle a new layer of security on my network....port knocking.

computerworld

Full Story :

http://www.computerworld.com.au/index.php/id;1702094698;fp;16;fpid;1

❖ Getting political

A recent U.S. government report entitled Annual Report to Congress on the Military Power of the People's Republic of China (PRC) 2008 talks extensively about the increasing role of China's ability to conduct war over the Internet. In the past, such talk of a "digital Pearl Harbor" has been dismissed by some security experts as largely political hot air. Yet more and more evidence suggests that a politically sponsored Internet event could occur sooner rather than later.

I spoke recently with Josh Corman, principal security strategist for IBM Internet Security Systems, who believes that criminal hackers follow three basic motivations: prestige, profit, and politics--the three Ps. It's the latter that he's concerned about. "All of our security defense models," said Corman, "were built based on a model of threat which was purely prestige driven," referring to the virus writer who only wanted his creation mentioned on the evening news.

Cnet reviews

Full Story :
http://reviews.cnet.com/4520-3513_7-6849578-1.html?part=rss&subj=edfeat&tag=Getting+political

New Vulnerabilities Tested in SecureScout

❖ 16896 Microsoft Office Memory Corruption Vulnerability (MS08-016/949030) (Remote File Checking)

A remote code execution vulnerability exists in the way Microsoft Office processes malformed Office files. An attacker could exploit the vulnerability by creating a malformed Office file which could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

If a user were logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

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

Some References:

* MS: MS08-016
http://www.microsoft.com/technet/security/bulletin/ms08-016.mspx
* CERT: TA08-071A
http://www.us-cert.gov/cas/techalerts/TA08-071A.html
* BID: 28146
http://www.securityfocus.com/bid/28146

* FRSIRT: ADV-2008-0848
http://www.frsirt.com/english/advisories/2008/0848/references
* SECUNIA: 29321
http://secunia.com/advisories/29321

CVE Reference: CVE-2008-0118

❖ 16895 Microsoft Office Cell Parsing Memory Corruption Vulnerability (MS08-016/949030) (Remote File Checking)

A remote code execution vulnerability exists in the way Microsoft Office handles specially crafted Excel files. An attacker could exploit the vulnerability by creating a malformed file which could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

If a user were logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

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

References:

* MS: MS08-016
http://www.microsoft.com/technet/security/bulletin/ms08-016.mspx
* CERT: TA08-071A
http://www.us-cert.gov/cas/techalerts/TA08-071A.html
* FRSIRT: ADV-2008-0848
http://www.frsirt.com/english/advisories/2008/0848/references
* SECUNIA: 29321
http://secunia.com/advisories/29321

CVE Reference: CVE-2008-0113

❖ 16894 Outlook URI Vulnerability (MS08-015/949031) (Remote File Checking)

A remote code execution exists in Outlook. The vulnerability could allow remote code execution if Outlook is passed a specially crafted mailto URI. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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:

* MS: MS08-015
http://www.microsoft.com/technet/security/bulletin/ms08-015.mspx
* CERT: TA08-071A
http://www.us-cert.gov/cas/techalerts/TA08-071A.html
* CERT-VN: VU#393305
http://www.kb.cert.org/vuls/id/393305
* BID: 28147
http://www.securityfocus.com/bid/28147
* FRSIRT: ADV-2008-0847
http://www.frsirt.com/english/advisories/2008/0847/references
* SECUNIA: 29320
http://secunia.com/advisories/29320

CVE Reference: CVE-2008-0110

❖ 16893 Excel Macro Validation Vulnerability (MS08-014/949029) (Remote File Checking)

A remote code execution vulnerability exists in the way Excel handles macros when opening specially crafted Excel files. An attacker could exploit the vulnerability by sending a malformed file which could be hosted on a specially crafted or compromised Web site, or included as an e-mail attachment.

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

References:

* CONFIRM:
http://www.microsoft.com/technet/security/advisory/947563.mspx
* MS: MS08-014
http://www.microsoft.com/technet/security/bulletin/ms08-014.mspx
* BID: 27305
http://www.securityfocus.com/bid/27305
* FRSIRT: ADV-2008-0146
http://www.frsirt.com/english/advisories/2008/0146
* FRSIRT: ADV-2008-0846
http://www.frsirt.com/english/advisories/2008/0846/references
* SECTRACK: 1019200
http://securitytracker.com/id?1019200
* SECUNIA: 28506
http://secunia.com/advisories/28506
* XF: microsoft-excel-unspecified-code-execution(39699)
http://xforce.iss.net/xforce/xfdb/39699

CVE Reference: CVE-2008-0081

❖ 16892 Excel Conditional Formatting Vulnerability (MS08-014/949029) (Remote File Checking)

A remote code execution vulnerability exists in the way Excel handles conditional formatting values. An attacker could exploit the vulnerability by sending a malformed file which could be hosted on a specially crafted or compromised Web site, or included as an e-mail attachment.

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

References:

* MS: MS08-014
http://www.microsoft.com/technet/security/bulletin/ms08-014.mspx
* CERT: TA08-071A
http://www.us-cert.gov/cas/techalerts/TA08-071A.html
* BID: 28170
http://www.securityfocus.com/bid/28170
* FRSIRT: ADV-2008-0846
http://www.frsirt.com/english/advisories/2008/0846/references

CVE Reference: CVE-2008-0117

❖ 16891 Excel Rich Text Validation Vulnerability (MS08-014/949029) (Remote File Checking)

A remote code execution vulnerability exists in the way Excel handles rich text values when loading application data into memory. An attacker could exploit the vulnerability by sending a malformed file which could be hosted on a specially crafted or compromised Web site, or included as an e-mail attachment.

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

References:

* MS: MS08-014
http://www.microsoft.com/technet/security/bulletin/ms08-014.mspx
* CERT: TA08-071A
http://www.us-cert.gov/cas/techalerts/TA08-071A.html
* BID: 28168
http://www.securityfocus.com/bid/28168
* FRSIRT: ADV-2008-0846
http://www.frsirt.com/english/advisories/2008/0846/references

CVE Reference: CVE-2008-0116

❖ 16890 Excel Formula Parsing Vulnerability (MS08-014/949029) (Remote File Checking)

A remote code execution vulnerability exists in the way Excel handles malformed formulas. An attacker could exploit the vulnerability by sending a malformed file which could be hosted on a specially crafted or compromised Web site, or included as an e-mail attachment.

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

References:

* MS: MS08-014
http://www.microsoft.com/technet/security/bulletin/ms08-014.mspx
* CERT: TA08-071A
http://www.us-cert.gov/cas/techalerts/TA08-071A.html
* BID: 28167
http://www.securityfocus.com/bid/28167
* FRSIRT: ADV-2008-0846
http://www.frsirt.com/english/advisories/2008/0846/references
* SECTRACK: 1019585
http://www.securitytracker.com/id?1019585

CVE Reference: CVE-2008-0115

❖ 16889 Excel Style Record Vulnerability (MS08-014/949029) (Remote File Checking)

A remote code execution vulnerability exists in the way Excel handles Style record data when opening Excel files. An attacker could exploit the vulnerability by sending a malformed file which could be hosted on a specially crafted or compromised Web site, or included as an e-mail attachment.

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

References:

* MS: MS08-014
http://www.microsoft.com/technet/security/bulletin/ms08-014.mspx
* CERT: TA08-071A
http://www.us-cert.gov/cas/techalerts/TA08-071A.html
* BID: 28166
http://www.securityfocus.com/bid/28166
* FRSIRT: ADV-2008-0846
http://www.frsirt.com/english/advisories/2008/0846/references

CVE Reference: CVE-2008-0114

❖ 16888 Excel File Import Vulnerability (MS08-014/949029) (Remote File Checking)

A remote code execution vulnerability exists in the way Excel handles data when importing files into Excel. An attacker could exploit the vulnerability by sending a malformed .slk file which could be hosted on a specially crafted or compromised Web site, or included as an e-mail attachment, and which could then be imported into Excel.

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

References:

* MS: MS08-014
http://www.microsoft.com/technet/security/bulletin/ms08-014.mspx
* CERT: TA08-071A
http://www.us-cert.gov/cas/techalerts/TA08-071A.html
* BID: 28095
http://www.securityfocus.com/bid/28095
* FRSIRT: ADV-2008-0846
http://www.frsirt.com/english/advisories/2008/0846/references

CVE Reference: CVE-2008-0112

❖ 16887 Excel Data Validation Record Vulnerability (MS08-014/949029) (Remote File Checking)

A remote code execution vulnerability exists in the way Excel processes data validation records when loading Excel files into memory. An attacker could exploit the vulnerability by sending a malformed file which could be hosted on a specially crafted or compromised Web site, or included as an e-mail attachment.

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

References:

* MS: MS08-014
http://www.microsoft.com/technet/security/bulletin/ms08-014.mspx
* CERT: TA08-071A
http://www.us-cert.gov/cas/techalerts/TA08-071A.html
* BID: 28094
http://www.securityfocus.com/bid/28094
* FRSIRT: ADV-2008-0846
http://www.frsirt.com/english/advisories/2008/0846/references

CVE Reference: CVE-2008-0111

New Vulnerabilities found this Week

Sun Java JDK / JRE Multiple Vulnerabilities

“Denial of Service”

Some vulnerabilities have been reported in Sun Java, which can be exploited by malicious people to cause a DoS (Denial of Service), to bypass certain security restrictions, or to compromise a vulnerable system.

1) Two unspecified errors in the Java Runtime Environment Virtual Machine can be exploited by a malicious, untrusted applet to read and write local files and execute local

applications.

2) An unspecified error in the Java Runtime Environment (JRE) when processing XSLT transformations can be exploited by untrusted applets or applications to e.g. read certain URL resources or potentially execute arbitrary code.

3) Three boundary errors exist in Java Web Start. These can be exploited e.g. by an untrusted Java Web Start application to read and write local files and execute local applications.

4) An unspecified error in Java Web Start can be exploited by a malicious, untrusted applet to read and write local files or execute local applications.

5) An unspecified error in Java Web Start can be exploited by an untrusted Java Web Start application to create files on the system and run local applications with the privileges of the user running the untrusted Java Web Start application.

6) An unspecified error in the Java Plug-in can be exploited by an applet to bypass the same origin policy and to execute local applications.

7) Some errors in the Java Runtime Environment image parsing library within the processing of ICC profiles can be exploited to crash the JVM or to write local files and execute local applications.

8) An error in the Java Runtime Environment may allow java script code within a browser to make connections through Java APIs to network services on the local system.

9) A boundary error exists in Java Web Start in the processing of JNLP files, which can be exploited to cause a stack-based buffer overflow when a user visits a malicious web site.

References:
http://java.sun.com/javase/6/webnotes/ReleaseNotes.html

RealPlayer ActiveX Control "Console" Property Memory Corruption
“Execute arbitrary code”

Elazar Broad has discovered a vulnerability in RealPlayer, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error within the RealPlayer ActiveX Control (rmoc3260.dll) when handling the "Console" property. This can be exploited to cause a memory corruption and execute arbitrary code when a user e.g. is tricked into visiting a malicious website.

The vulnerability is confirmed in RealPlayer version 11.0.1 (build 6.0.14.794) including rmoc3260.dll version 6.0.10.45. Other versions may also be affected.

References:
http://lists.grok.org.uk/pipermail/full-disclosure/2008-March/060659.html

MailEnable SMTP Service EXPN/VRFY Denial of Service Vulnerabilities
“Denial of Service”

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

The vulnerabilities are caused due to boundary errors within the SMTP service (MESMTPC.exe) when handling EXPN or VRFY commands. These can be exploited to cause the service to crash via a specially crafted EXPN or VRFY command.

The vulnerability reportedly affects all versions.

References:
http://www.mailenable.com/hotfix/

MailEnable IMAP Service Multiple Vulnerabilities

"Denial of Service; Execution of arbitrary code"

Luigi Auriemma has discovered some vulnerabilities in MailEnable, which can be exploited by malicious people and malicious users to cause a DoS (Denial of Service) or by malicious users to compromise a vulnerable system.

1) Boundary errors in the IMAP service (MEIMAPS.EXE) when handling arguments passed to the FETCH, EXAMINE, and UNSUBSCRIBE commands can be exploited to cause buffer overflows via overly long arguments.

Successful exploitation allows execution of arbitrary code.

2) Errors in the IMAP service when handling the SEARCH and APPEND commands can be exploited to cause the service to crash.

The vulnerabilities are confirmed in MailEnable Professional version 3.13. Other versions may also be affected.

References:
http://aluigi.altervista.org/adv/maildisable-adv.txt

Check Point VPN-1 UTM Edge Cross-Site Scripting Vulnerability

"cross-site scripting"

Henri Lindberg has reported a vulnerability in Check Point VPN-1 UTM Edge, which can be exploited by malicious people to conduct cross-site scripting attacks.

Input passed to the "user" parameter in the login page is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of the web interface of the device.

The vulnerability is reported in Check Point VPN-1 Edge with Embedded NGX version 7.0.48x. Other versions may also be affected.

References:
http://www.louhi.fi/advisory/checkpoint_080306.txt

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