netVigilance

ScoutNews Team **12 November 2004**
Issue #46

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Trojans are becoming sneakier as they lurk in the background waiting for the right event and they are now also being used to SPAM cell phone SMS services or even cause DDoS attacks in very targeted ways.
At the same time establishing a security baseline is proving very difficult for the world largest software producer.

Enjoy reading

Top Security News Stories this Week

❖ Sneakier Trojan Targets UK Banks

A disturbingly crafty Trojan is targeting banking consumers. This malware does not mimic the standard phishing attacks that attempt to trick a user into logging onto a fake Web site designed to look like the bank's, Sophos security consultant Graham Cluley tells NewsFactor. Instead, "it lurks in the background of a user's computer waiting for him or her to visit a banking Web site. When that happens, the Trojan gathers the passwords and even takes screen shots of the pages, and then sends them back to the hackers." The hackers, of course, avail themselves of the data and raid the user's bank account.
http://story.news.yahoo.com/news?tmpl=story&ncid=1212&e=4&u=/nf/20041112/tc_nf/28350&sid=95573505
Erika Morphy *www.enterprise-security-today.com*

❖ Security Firm Reports Ten New XP SP2 Flaws

A security firm says it has found 10 major security flaws in Microsoft's Windows XP Service Pack 2. The weaknesses could allow intruders to bypass many of the security measures implemented by the update.
A hacker could exploit the flaws to execute malicious code on a user's system by luring the user to a specially created Web page, according to Finjan Software, which reported the vulnerability.
http://story.news.yahoo.com/news?tmpl=story&ncid=1209&e=4&u=/nf/20041112/tc_nf/28377&sid=95573734
Robin Arnfield, www.newsfactor.com

- Trojan invades Russian mobiles
  Moscow burns

A TROJAN HORSE with a name that takes over a PC so that it sends SMS spam to mobile phones has been spotted in Russia.

The Delf-HA Trojan contacts a Web site for details on which spam campaign to run and then randomly generates a series of Russian mobile numbers beginning with the prefix +7921 or +7911. It logs into the SMS sites of the Russian mobile phone companies to distribute the campaign.

http://www.theinquirer.net/?article=19613

Nick Farrell

New Vulnerabilities Tested in SecureScout

- **14474 Mozilla Firefox Multiple Vulnerabilities**

Details have been released about several vulnerabilities in Mozilla Firefox. These can potentially be exploited to detect the presence of local files, cause a DoS (Denial of Service), disclose sensitive information, spoof the file download dialog, and gain escalated privileges.

1) Web sites may include images from local resources, which can be exploited to determine the existence of local images, cause a DoS by referencing device files (e.g. "/dev/tty0"), and potentially steal passwords from Windows systems via file shares.

2) The file download dialog box truncates filenames, which potentially can be exploited to spoof file extensions in the file download dialog.

3) On Mac OS X, Firefox is installed with world-writable permissions, which potentially can be exploited by malicious, local users to gain escalated privileges.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://www.mozilla.org/security/ & http://www.securityfocus.org/bid/10681/info/

- **14668 Vulnerability in ISA Server 2000 and Proxy Server 2.0 Could Allow Internet Content Spoofing (MS04-039/888258)**

This is a spoofing vulnerability that exists in the affected products and that could enable an attacker to spoof trusted Internet content. Users could believe they are accessing trusted Internet content when in reality they are accessing malicious Internet content, for example a malicious Web site. However, an attacker would first have to persuade a user to visit the attacker’s site to attempt to exploit this vulnerability.

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

CVE Links: CAN-2004-0892

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-039.mspx

- **15561 MIME buffer overflow in Sendmail 8.8.0 and 8.8.1 gives root access**

Sendmail versions 8.8.0 and 8.8.1 are vulnerable to a buffer overflow in the MIME processing code. A remote attacker can overflow a buffer and execute arbitrary commands on the system to root privileges. This vulnerability is similar but unrelated to the MIME overflow in 8.8.3/8.8.4. Exploit information for this vulnerability is widespread.

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

CVE Links: CVE-1999-0206

Reference: http://xforce.iss.net/xforce/xfdb/1836 &http://www.sendmail.org & http://icat.nist.gov/icat.cfm?cvename=CVE-1999-0206

❖ 15562 Sendmail ETRN commands denial of service vulnerability

Sendmail before 8.10.0 allows remote attackers to cause a denial of service by sending a series of ETRN commands then disconnecting from the server, while Sendmail continues to process the commands after the connection has been terminated.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS** Risk: **High**

CVE Link: CVE-1999-1109

Reference: http://marc.theaimsgroup.com/?l=bugtraq&m=94632241202626&w=2 & http://www.sendmail.org & http://icat.nist.gov/icat.cfm?cvename=CVE-1999-1109

❖ 15563 Sendmail mail.local Vulnerabilities

The mail.local program in Sendmail version 8.9.3 is vulnerable to a denial of service attack. The program, which is a local mail delivery agent in Sendmail, fails to properly identify the ".\n" end of message string. A remote attacker can crash the mail server or corrupt mailboxes by sending a long string of 2047 or more characters that ends with ".\n".

Test Case Impact: **Gather info** Vulnerability Impact: **DoS** Risk: **High**

CVE Link: CVE-2000-0319

Reference: http://www.securityfocus.com/bid/1146/discussion/ & http://www.sendmail.org & http://icat.nist.gov/icat.cfm?cvename=CVE-2000-0319

❖ 15564 Sendmail race conditions in signal handlers vulnerability

Sendmail before 8.11.4, and 8.12.0 before 8.12.0.Beta10, allows local users to cause a denial of service and possibly corrupt the heap and gain privileges via race conditions in signal handlers.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS** Risk: **High**

CVE Link: CVE-2001-1349

Reference: http://archives.neohapsis.com/archives/sendmail/2001-q2/0001.html & http://www.sendmail.org

❖ 15532 "Established" Keyword May Allow Packets to Bypass Filter (CSCdi34061)

There is a vulnerability in Cisco's IOS software when the 'established' keyword is used in extended IP access control lists. This bug can, under very specific circumstances and only with certain IP host implementations, allow unauthorized packets to circumvent a filtering router.

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

CVE Link: CVE-1999-0162

Reference:
http://www.cisco.com/en/US/products/products_security_advisory09186a00800b13b9.shtml

❖ 15533 Incorrectly Parsed Access-list May Allow Packets to Bypass Filter (CSCdi36962)

A bug in certain versions of IOS can cause extended IP access lists to be parsed incorrectly. Under some circumstances, this may allow packets to bypass IP packet filtering. This may permit unintended IP traffic to pass through a filtering router.

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

CVE Link: CVE-1999-0161

Reference:
http://www.cisco.com/en/US/products/products_security_advisory09186a00800b1386.

❖ 15534 Possible Access Control Bypass and Denial of Service in Gigabit Switch Routers Using Gigabit Ethernet or Fast Ethernet Cards (CSCdp35794)

Software running on all models of Gigabit Switch Routers (GSRs) configured with Gigabit Ethernet or Fast Ethernet cards may cause packets to be forwarded without correctly evaluating configured access control lists (ACLs). In addition to circumventing the access control lists, it is possible to stop an interface from forwarding any packets, thus causing a denial of service.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS** Risk: **High**

CVE Link: CVE-1999-0162

Reference:
http://www.cisco.com/en/US/products/products_security_advisory09186a00800b1392.shtml

❖ 15536 Cisco IOS Software TCP Initial Sequence Number Randomization Improvements (CSCds04747)

There is a vulnerability in Cisco's IOS software when the 'established' keyword is used in extended IP access control lists. This bug can, under very specific circumstances and only with certain IP host implementations, allow unauthorized packets to circumvent a filtering router.

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

CVE Link: CAN-2001-0328

Reference:
http://www.cisco.com/en/US/products/products_security_advisory09186a00800b13b9.shtml

New Vulnerabilities found this Week

- **SquirrelMail Encoded Headers Script Insertion Vulnerability**
"Script insertion attacks"

Joost Pol has reported a vulnerability in SquirrelMail, which can be exploited by malicious people to conduct script insertion attacks.
The vulnerability is caused due to an input validation error in the "decodeHeader()" function in "mime.php" when processing encoded text in headers. This can be exploited to inject arbitrary HTML and script code, which will be executed in a user's browser session in context of a vulnerable site.
The vulnerability has been reported in the following versions:
* SquirrelMail 1.4.3a and prior
* SquirrelMail 1.5.1-cvs before 23rd October 2004

References: http://prdownloads.sourceforge.n...relmail/sm143a-xss.diff?download

- **Cisco IOS DHCP Packet Handling Denial of Service Vulnerability**
"Denial of Service"

A vulnerability has been reported in Cisco IOS, which can be exploited by malicious people to cause a DoS (Denial of Service).
The vulnerability is caused due to an error within the processing of DHCP packets. This can be exploited to block the input queue on an interface by sending some specially crafted DHCP packets to a vulnerable device.
Successful exploitation requires that the DHCP server or relay agent is enabled (default setting), but not necessarily configured.
The following products running Cisco IOS version 12.2(14)SZ or a variant of Cisco IOS 12.2(18)S and higher are affected:
* Cisco 7200, 7300, 7500 platforms
* Cisco 2650, 2651, 2650XM, 2651XM Multiservice platform
* Cisco ONS15530, ONS15540
* Cisco Catalyst 4000, Sup2plus, Sup3, Sup4 and Sup5 modules
* Cisco Catalyst 4500, Sup2Plus TS
* Cisco Catalyst 4948, 2970, 3560, and 3750
* Cisco Catalyst 6000, Sup2/MSFC2 and Sup720/MSFC3
* Cisco 7600 Sup2/MSFC2 and Sup720/MSFC3

References:
http://www.cisco.com/warp/public/707/cisco-sa-20041110-dhcp.shtml
http://www.kb.cert.org/vuls/id/630104

- **Mozilla Firefox Multiple Vulnerabilities**

"Detect the presence of local files, cause a DoS (Denial of Service), disclose sensitive information, spoof the file download dialog, and gain escalated privileges"
Details have been released about several vulnerabilities in Mozilla Firefox. These can potentially be exploited to detect the presence of local files, cause a DoS (Denial of Service), disclose sensitive information, spoof the file download dialog, and gain escalated privileges.
1) Web sites may include images from local resources, which can be exploited to determine the existence of local images, cause a DoS by referencing device files (e.g. "/dev/tty0"), and potentially steal passwords from Windows systems via file shares.
2) The file download dialog box truncates filenames, which potentially can be exploited to spoof file extensions in the file download dialog.
3) On Mac OS X, Firefox is installed with world-writable permissions, which potentially can be exploited by malicious, local users to gain escalated privileges.

References:
https://bugzilla.mozilla.org/show_bug.cgi?id=69070
https://bugzilla.mozilla.org/show_bug.cgi?id=234416
https://bugzilla.mozilla.org/show_bug.cgi?id=261527

- **Linux Kernel ELF Binary Loader Setuid File Handling Vulnerabilities**

"Gain escalated privileges"
Paul Starzetz has reported some vulnerabilities in the Linux kernel, which potentially can be exploited by malicious, local users to gain escalated privileges.
The vulnerabilities are caused due to various errors within the Linux ELF binary loader when handling setuid binaries.
Successful exploitation may potentially allow execution of arbitrary code with root privileges.
The vulnerability affects the following versions:
* Linux kernel 2.4 branch up to to and including 2.4.27
* Linux kernel 2.6 branch up to to and including 2.6.8
Other versions may also be affected.

References: http://www.isec.pl/vulnerabilities/isec-0017-binfmt_elf.txt

- **Microsoft ISA Server / Proxy Server Internet Content Spoofing Vulnerability**

"Spoof Internet content"
Martijn de Vries and Thomas de Klerk have reported a vulnerability in Microsoft ISA Server 2000 and Proxy Server 2.0, which can be exploited by malicious people to spoof Internet content.
The vulnerability is caused due to an error within the method used for caching results of reverse lookups. The problem is that reverse lookups results are used for forward lookups.
This can be exploited by making the server perform a reverse lookup for an IP address and then supply a spoofed reverse lookup response for an arbitrary domain name.
Successful exploitation poisons the DNS cache and may result in users unknowingly accessing malicious web sites when attempting to access a trusted web site.
NOTE: Exploitation does not allow spoofing of SSL certificates on HTTPS sites.

References: http://www.microsoft.com/technet/security/bulletin/MS04-039.mspx

- **Samba Wildcard Filename Matching Denial of Service Vulnerability**

  "Denial of Service"

Karol Wiesek has reported a vulnerability in Samba, which can be exploited by malicious users to cause a DoS (Denial of Service).
The vulnerability is caused due to an input validation error within the "ms_fnmatch()" function when matching filenames containing wildcard characters. This can be exploited via multiple specially crafted commands to consume a large amount of CPU resources.
Successful exploitation may cause the server to stop responding entirely.
The vulnerability affects version 3.0.7 and prior.

References: http://us1.samba.org/samba/security/CAN-2004-0930.html

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