netVigilance

ScoutNews Team **22 October 2004**
Issue #43

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Major vulnerabilities and loopholes found in almost all mainstream antivirus products!!
The verdict is out – Blended attacks are more dangerous than anything else and at the same time Ballmer is predicting that hackers are getting smarter.

Enjoy reading

Top Security News Stories this Week

- **Anti-Virus Can Be Tricked By Hackers**

The anti-virus detection engines of several big-name vendors, including McAfee and Computer Associates, can be fooled by hackers, a U.S.-based security intelligence firm warned Tuesday.
According to an advisory posted by iDefense, a Reston, Va.-based vulnerability intelligence provider, the bug could let hackers slip their malicious code past the anti-virus defenses thrown up by McAfee, Computer Associates, Kaspersky Labs, Sophos, Eset, and RAV. (The last in the list, RAV, is the anti-virus technology that Microsoft acquired in 2003.)
http://www.internetweek.com/breakingNews/showArticle.jhtml;jsessionid=B5QBDHHFBOJ0QQSNDBGCKHSCJUMEKJVN?articleID=50500905
TechWeb News

- **Merging of viruses and spam maximizes damage**

When the SoBig.A virus first appeared in January 2003, I doubt many security experts looking at it predicted its enormous significance. A year on, the SoBig family of viruses has entered folklore as the most virulent strain of a new type of e-mail security threat.
http://www.biosmagazine.co.uk/op.php?id=176
Mark Sunner

- **Microsoft CEO: Hackers Getting Smarter**

Microsoft Corp.'s chief executive believes it's naive to suggest the software giant can eliminate all security vulnerabilities in its various products even though engineers are trying hard to do so.

Hackers get smarter, too, Steve Ballmer told several thousand information-technology workers at the Gartner Symposium ITXPO.
But Ballmer said engineers were making progress, such as adding security enhancements to Windows Server 2003 when its next big update, Service Pack 1, comes out.
http://www.620ktar.com/news/article.aspx?id=481086
Mike Schneider

New Vulnerabilities Tested in SecureScout

- **13176 AOL Instant Messenger (AIM) Installed (Remote File Checking)**
  The remote host is using AOL Instant Messenger (AIM) - a p2p software, which may not be suitable for a business environment.

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

CVE Links:

Reference: http://www.aim.com/get_aim/win/latest_win.adp

- **13177 AOL Instant Messenger aim:goaway URI Handler Buffer Overflow Vulnerability (Remote File Checking)**
  The remote host is using AOL Instant Messenger (AIM) - a p2p software, which may not be suitable for a business environment.
  A buffer overflow error exists in the way that some versions of the AIM client software handle AIM 'Away' messages. This error creates a vulnerability that can be exploited by remote attackers supplying overly long input to the goaway function of the aim: URI handler. Exploitation of this vulnerability requires an AIM user to click on a malicious URL supplied in an instant message or embedded in a web page.

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

CVE Links: CAN-2004-0636

Reference: http://www.aim.com/get_aim/win/latest_win.adp & http://secunia.com/advisories/12198/ & http://www.kb.cert.org/vuls/id/735966

- **14665 Vulnerability in Windows Shell Could Allow Remote Code Execution (MS04-037/841356) (Remote File Checking)**
  If a user is logged on with administrative privileges, an attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges. However, user interaction is required to exploit these vulnerabilities.

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

CVE Links: CAN-2004-0214 & CAN-2004-0572

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-037.mspx

- **14666 Cumulative Security Update for Internet Explorer (MS04-038/834707) (Remote File Checking)**

If a user is logged on with administrative privileges, an attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

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

CVE Link: CAN-2004-0842 & CAN-2004-0727 & CAN-2004-0216 & CAN-2004-0839 & CAN-2004-0844 & CAN-2004-0843 & CAN-2004-0841 & CAN-2004-0845

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-038.mspx

- **15525 Exim 3.x - 4.x - EHLO/HELO Remote Heap Corruption Vulnerability**

Exim is a Unix message transfer agent (MTA) developed at the University of Cambridge. A heap corruption vulnerability has been discovered in Exim. The problem occurs due to insufficient bounds checking when handling user-supplied SMTP EHLO/HELO data. As a result, it may be possible to overrun the bounds of a heap memory buffer. Although it is believed to be unlikely, this could theoretically be exploited to execute arbitrary code with the privileges of Exim. It may also be possible to trigger a denial of service condition.

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

CVE Link: CVE-2001-0889

Reference: http://www.exim.org/ & http://www.securityfocus.com/archive/1/246345 & http://www.securityfocus.com/bid/3728/

- **15529 Exim 3.x - 4.x - Header Syntax Checking Remote Stack Buffer Overrun Vulnerability**

Exim is a Unix message transfer agent (MTA) developed at the University of Cambridge. Exim is reportedly prone to a remotely exploitable stack-based buffer overrun vulnerability.
This issue is exposed if header syntax checking has been enabled in the agent and may be triggered by a malicious e-mail. Though not confirmed to be exploitable, if this condition were to be exploited, it would result in execution of arbitrary code in the context of the mail transfer agent. Otherwise, the agent would crash when handling malformed syntax in an e-mail message.
It should be noted that the vulnerable functionality is not enabled in the default install, though some Linux/Unix distributions that ship the software may enable it by default.

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

CVE Link: CAN-2004-0400

Reference: http://www.exim.org/ & http://www.securityfocus.com/bid/10291/ & http://www.securityfocus.com/advisories/6683

- **15530 Exim 3.x Sender Verification Remote Stack Buffer Overrun Vulnerability**

Exim is a Unix message transfer agent (MTA) developed at the University of Cambridge. Exim has been reported prone to a remotely exploitable stack-based buffer overrun vulnerability.
This is exposed if sender verification has been enabled in the agent and may be triggered by a malicious e-mail. Exploitation may permit execution of arbitrary code in the content of the mail transfer agent.
This issue is reported in exist in Exim 3.35. Earlier versions may also be affected.
It should be noted that the vulnerable functionality is not enabled in the default install, though some Linux/Unix distributions that ship the software may enable it by default.

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

CVE Link: CAN-2004-0399

Reference: http://www.exim.org/ & http://www.securityfocus.com/bid/10290/

- **15531 Exim 3.x Pipe Hostname Arbitrary Command Execution Vulnerability**

Exim is a Unix message transfer agent (MTA) developed at the University of Cambridge.

When Exim receives a mail, it processes the mail by it's localhost and domain name. In the event that the mail contains a pipe (|) symbol as the first part of it's host name, Exim attempts to interpret the localhost name as a command. This could result in a mail with a maliciously crafted From: field being used to execute a command contained within the localhost name of the mailing host. This problem only affects configurations that routes or directs mail without performing any type of check on the local part of the address, and does not affect alias or forward files.

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

CVE Link: CVE-2001-0889

Reference: http://www.exim.org/ & http://www.securityfocus.com/archive/1/246345 & http://www.securityfocus.com/bid/3728/

- **17924 Apache 2 Basic authentication bypass**

A flaw in Apache 2.0.51 (only) broke the merging of the Satisfy directive which could result in access being granted to resources despite any configured authentication.

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

CVE Link: CAN-2004-0811

Reference: http://cve.mitre.org/cgi-bin/cvename.cgi?name=Cve-2004-0811 & http://www.apacheweek.com/features/security-20

- **17925 Apache 2 SSLCipherSuite bypass**
  An issue has been discovered in the mod_ssl module when configured to use the "SSLCipherSuite" directive in directory or location context. If a particular location context has been configured to require a specific set of cipher suites, then a client will be able to access that location using any cipher suite allowed by the virtual host configuration.

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

CVE Link: CAN-2004-0885

Reference: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0885 & http://www.apacheweek.com/features/security-20

New Vulnerabilities found this Week

- **Speedtouch USB Driver Privilege Escalation Vulnerability**
  "Gain escalated privileges"
  A vulnerability has been reported in Speedtouch USB Driver, which potentially can be exploited by malicious, local users to gain escalated privileges.
  The vulnerability is caused due to an unspecified format string errors in "modem_run", "pppoa2", and "pppoa3".
  Successful exploitation may potentially allow execution of arbitrary code with escalated privileges.
  References: http://speedtouch.sourceforge.net/index.php?/news.en.html

- **mpg123 "getauthfromURL()" Buffer Overflow Vulnerability**
  "Allow execution of arbitrary code"
  Carlos Barros has reported a vulnerability in mpg123, which potentially can be exploited by malicious people to compromise a user's system.
  The vulnerability is caused due to a boundary error in the "getauthfromURL()" function when parsing URLs. This can be exploited to cause a buffer overflow when a user e.g. loads a specially crafted playlist containing an overly long URL.
  Successful exploitation may potentially allow execution of arbitrary code.
  The vulnerability has been reported in versions pre0.59s and 0.59r. Other versions may also be affected.
  References: http://secunia.com/advisories/12908/

- **Linux Kernel Firewall Logging Rules Denial of Service Vulnerability**
  "Crash a vulnerable system"
  Richard Hart has reported a vulnerability in the Linux Kernel, which can be exploited by malicious people to cause a DoS (Denial of Service).
  The vulnerability is caused due to an integer underflow error within the iptables firewall logging rules. This can be exploited to crash a vulnerable system via a specially crafted

IP packet.
Successful exploitation requires that firewalling is enabled.
References: http://www.suse.de/de/security/2004_37_kernel.html

❖ **Microsoft Internet Explorer Two Vulnerabilities**

"Bypass a security feature in Microsoft Windows XP SP2"
http-equiv has discovered two vulnerabilities in Internet Explorer, which can be exploited by malicious people to compromise a user's system, link to local resources, and bypass a security feature in Microsoft Windows XP SP2.
1) Insufficient validation of drag and drop events from the "Internet" zone to local resources for valid images or media files with embedded HTML code. This can be exploited by e.g. a malicious web site to plant arbitrary HTML documents on a user's system, which may allow execution of arbitrary script code in the "Local Computer" zone.
NOTE: Microsoft Windows XP SP2 does not allow Active Scripting in the "Local Computer" zone.
2) A security zone restriction error, where an embedded HTML Help control on e.g. a malicious web site references a specially crafted index (.hhk) file, can execute local HTML documents.
NOTE: This will also bypass the "Local Computer" zone lockdown security feature in SP2.
The two vulnerabilities in combination with an inappropriate behaviour where the ActiveX Data Object (ADO) model can write arbitrary files can be exploited to compromise a user's system. This has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2.
References: http://support.microsoft.com/default.aspx?scid=kb;en-us;q154036

❖ **Gaim MSN SLP Message Handling Buffer Overflow Vulnerability**

"Buffer overflow"
A vulnerability has been reported in Gaim, which potentially can be exploited by malicious people to compromise a user's system.
The vulnerability is caused due to a boundary error within the handling of MSN SLP messages. This can be exploited to cause a buffer overflow by supplying a specially crafted sequence of MSN SLP messages.
Successful exploitation may potentially allow execution of arbitrary code.
Two other bugs have also been reported, which can be exploited to crash the application when accepting file transfers and processing a malformed MSN SLP message.
References:
http://gaim.sourceforge.net/security/index.php?id=9
http://gaim.sourceforge.net/security/index.php?id=8
http://gaim.sourceforge.net/security/index.php?id=7

❖ **RAV Antivirus Zip Archive Virus Detection Bypass Vulnerability**
❖ **NOD32 Antivirus Zip Archive Virus Detection Bypass Vulnerability**
❖ **eTrust Antivirus Zip Archive Virus Detection Bypass Vulnerability**
❖ **McAfee Anti-Virus Zip Archive Virus Detection Bypass Vulnerability**
❖ **Sophos Anti-Virus Zip Archive Virus Detection Bypass**
❖ **Kaspersky Anti-Virus Zip Archive Virus Detection Bypass Vulnerability**
❖ **Twister Anti-TrojanVirus MS-DOS Device Name Handling Weakness**

A vulnerability has been reported in multiple Anti-Virus Engines, which can be exploited

by malware to bypass certain scanning functionality.
The vulnerability is caused due to an error when parsing .zip archive headers and can be exploited via a specially crafted .zip archive where the uncompressed size of the archived file has been modified within the local and global headers.
Successful exploitation causes malware in a specially crafted .zip archive to pass the scanning functionality undetected.
NOTE: This is not a critical issue on client systems, as the malware still is detected upon execution by the antivirus on-access scanner.
References: http://www.idefense.com/applicat...?id=153&type=vulnerabilities

- **Windows XP Internet Connection Firewall Bypass Weakness**

A weakness has been reported in Windows XP, which can be exploited to bypass certain rules in the Internet Connection Firewall (ICF).
The problem is caused due to the firewall by default accepting incoming connections to ports listened on by the "sessmgr.exe" process.
This can e.g. be exploited by malicious, unprivileged users to host an unauthorized service or by a trojan to accept incoming connections by starting "sessmgr.exe" and then inject malicious code into the running process.
Successful exploitation does not require administrative privileges on an affected system.
The weakness has been reported in Windows XP SP2. Other versions may also be affected.
NOTE: This is a general problem with personal firewalls and can be exploited via any program granted access through the firewall without user interaction. It is a known issue and have been discussed in the security community about 2 years ago. PoC exploit code has also priorly been released by Oliver Lavery.
References: http://secunia.com/advisories/12793/

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