netVigilance

ScoutNews Team **November 4, 2005**
Issue # 44

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

October fest for virus writers, anti-virus for mobile phones, Cisco announces patch for infamous Blackhat vulnerability, DoS attacks are OK in the UK and AOL rootkit worm emerges.

Enjoy reading and Stay Vigilant!

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

- **October yields big virus harvest**

Sophos reports that a staggering 1,685 new viruses were written in October. This represents a record number of new viruses for a single month since Sophos started keeping track of this information in the late 80's.

The viruses all come from 3 families; Mytob, Netsky and Zafi. Mytob variants made up 2/3 of the new viruses.

CRN

Full Story:

http://www.enterpriseitplanet.com/security/news/article.php/3561686

❖ Aladdin rolls anti-virus for cell phones

Aladdin Knowledge Systems announced the release of e-safe MCSG anti-virus for Symbian, J2ME, PalmOS, and Windows Mobile/CE based mobile devices.

In addition to anti-virus, e-safe also contains anti-spyware, Spam management and application filtering.

Related Links:
http://www.aladdin.com/news/2005/eSafe/eSafe_MMS.asp

❖ Cisco releases patch for 'Blackhat' flaw

More on the Cisco IOS vulnerability presented by Michael Lynn at this years' Blackhat conference. Cisco released a patch for specific versions of IOS that are affected by the much publicized flaw that caused many to lose their heads and one security engineer to lose his job. (Scout News #30, #31)

Products affected by the heap overflow issue include Cisco IOS 12.0 through 12.4.
Yahoo

Full Story:
http://news.yahoo.com/s/zd/20051103/tc_zd/164318

❖ Teen scot-free in UK DoS attack case

A British teenager accused of sending millions of emails to his employer causing a Denial of Service (DoS) attack, goes free under British law.

The 1990 Computer Misuse Act apparently does not address DoS type attacks since they do not constitute "unauthorized access to or modification of computer systems." Even though damages from a DoS attack could run in the millions of dollars for a large organization; the law contains a gaping loophole .
BBC

Full Story:
http://news.bbc.co.uk/1/hi/technology/4402572.stm

❖ First rootkit exploit hits AOL users

History is made again, a dangerous Worm is spreading through AOL instant messenger (AIM) network; installing a rootkit on the users PC.

This alarming trend represents the first ever piece of very serious malware that can be spread by an instant messaging application.
CRN

Full Story:
http://www.newsfactor.com/news/New-Worm-Targets-AOL-Messenger/story.xhtml?story_id=13300CYE9CDW

New Vulnerabilities Tested in SecureScout

- **12110 Microsoft SQL Server Monitor Buffer Overflow Vulnerability (ssnetlib.dll version check)**

Microsoft SQL Server is a very widely used SQL server.
Besides the SQL Server port 1433, this software has a service called SQL Server Resolution Service (SSRS) listening on the UDP port 1434.

It is possible to perform a buffer overflow attack by sending crafted packets.

This vulnerability could be exploited to run arbitrary code on your server.

Please note that authentication is not required, which makes this vulnerability easier to exploit.

A worm (called w32.slammer or Sapphire) exploiting this vulnerability appeared in late January 2003.

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

References:

@NO-MS02-039@
@NO-MS02-061@
Initial advisory: http://www.nextgenss.com/advisories/mssql-udp.txt
CERT Advisory CA-2002-22: http://www.cert.org/advisories/CA-2002-22.html
CERT Vulnerability Note VU#484891: http://www.kb.cert.org/vuls/id/484891
Threat Profiling Microsoft SQL Server: http://www.nextgenss.com/papers/tp-SQL2000.pdf
Microsoft Security Bulletin MS02-039:
http://www.microsoft.com/technet/security/bulletin/MS02-039.asp
Microsoft Security Bulletin MS02-061 version 2:
http://www.microsoft.com/technet/security/bulletin/MS02-061.asp
Analysis of Sapphire worm: http://www.techie.hopto.org/sqlworm.html
CERT Advisory CA-2003-04 on related worm: http://www.cert.org/advisories/CA-2003-04.html

Microsoft Aller on worm:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/virus/alerts/slammer.asp
SANS Top 20 Microsoft SQL Server (MSSQL): http://www.sans.org/top20/#W2
SANS Top 20 Windows Remote Access Services: http://www.sans.org/top20/#W5

CVE Reference: CAN-2002-0649

❖ 13306 Oracle Database Server - Oracle Label Security component Unspecified error (oct-2005/DB15)

An unspecified error in the Oracle Label Security component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

Product Homepage:
http://www.oracle.com/

CVE Reference: CAN-2005-0873

❖ 13307 Oracle Database Server - Oracle Security Service component Unspecified error (oct-2005/DB16)

An unspecified error in the Oracle Security Service component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.
Test Case Impact: **Gather Info.** Vulnerability Impact: **High** Risk: **Attack**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

Product Homepage:
http://www.oracle.com/

CVE Reference: CAN-2005-0873

❖ 13308 Oracle Database Server - Oracle Spatial component Unspecified error (oct-2005/DB17)

An unspecified error in the Oracle Spatial component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

Product Homepage:
http://www.oracle.com/

CVE Reference: CAN-2005-0873

❖ 16025 PHP GLOBALS array is not properly protected Vulnerability

A vulnerability has been reported in PHP, which can be exploited by malicious people to conduct cross-site scripting attacks, bypass certain security restrictions, and potentially compromise a vulnerable system.

An error where the "GLOBALS" array is not properly protected, can be exploited to define global variables by sending a "multipart/form-data" POST request with a specially crafted file upload field, or via a script calling the PHP function "extract()" or "import_request_variables()".

Successful exploitation may open up for vulnerabilities in various applications, but requires that "register_globals" is enabled.

The vulnerability has been reported in versions 4.4.0 and 5.0.5, and prior

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

References:

Advisory:
http://www.hardened-php.net/advisory_202005.79.html
http://www.hardened-php.net/advisory_192005.78.html
http://www.hardened-php.net/advisory_182005.77.html
http://www.hardened-php.net/index.76.html
http://www.php.net/release_4_4_1.php

Other references:
http://secunia.com/advisories/17371/

Product Page:
http://www.php.net/

CVE Reference: CAN-2005-2491

❖ 16026 PHP unexpected termination in the "parse_str()" Vulnerability

A vulnerability has been reported in PHP, which can be exploited by malicious people to conduct cross-site scripting attacks, bypass certain security restrictions, and

potentially compromise a vulnerable system.

An error in the handling of an unexpected termination in the "parse_str()" PHP function, can be exploited to enable the "register_globals" directive for the current execution by e.g. triggering a memory_limit request shutdown in a script calling "parse_str()".

The vulnerability has been reported in versions 4.4.0 and 5.0.5, and prior.

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

References:

Advisory:
http://www.hardened-php.net/advisory_202005.79.html
http://www.hardened-php.net/advisory_192005.78.html
http://www.hardened-php.net/advisory_182005.77.html
http://www.hardened-php.net/index.76.html
http://www.php.net/release_4_4_1.php

Other references:
http://secunia.com/advisories/17371/

Product Page:
http://www.php.net/

CVE Reference: CAN-2005-2491

❖ 16027 PHP input passed to the "phpinfo()" PHP function not properly sanitized Vulnerability

A vulnerability has been reported in PHP, which can be exploited by malicious people to conduct cross-site scripting attacks, bypass certain security restrictions, and potentially compromise a vulnerable system.

Some unspecified input passed to the "phpinfo()" PHP function isn't properly sanitised before being returned to the user. This can be exploited via a script calling "phpinfo()" to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerability has been reported in versions 4.4.0 and 5.0.5, and prior.

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

References:

Advisory:
http://www.hardened-php.net/advisory_202005.79.html
http://www.hardened-php.net/advisory_192005.78.html
http://www.hardened-php.net/advisory_182005.77.html
http://www.hardened-php.net/index.76.html
http://www.php.net/release_4_4_1.php

Other references:

http://secunia.com/advisories/17371/

Product Page:
http://www.php.net/

CVE Reference: CAN-2005-2491

❖ 16028 PHP integer overflow error in pcrelib Vulnerability

A vulnerability has been reported in PHP, which can be exploited by malicious people to conduct cross-site scripting attacks, bypass certain security restrictions, and potentially compromise a vulnerable system.

An integer overflow error in pcrelib may be exploited to cause a memory corruption via a script calling a PHP function using the PCRE library where the regular expression can be controlled by the attacker.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been reported in versions 4.4.0 and 5.0.5, and prior.

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

References:

Advisory:
http://www.hardened-php.net/advisory_202005.79.html
http://www.hardened-php.net/advisory_192005.78.html
http://www.hardened-php.net/advisory_182005.77.html
http://www.hardened-php.net/index.76.html
http://www.php.net/release_4_4_1.php

Other references:
http://secunia.com/advisories/17371/

Product Page:
http://www.php.net/

CVE Reference: CAN-2005-2491

❖ 16029 PHP bypass the "safe_mode" and "open_basedir" protection mechanisms Vulnerability

A vulnerability has been reported in PHP, which can be exploited by malicious people to conduct cross-site scripting attacks, bypass certain security restrictions, and potentially compromise a vulnerable system.

The problem is that it is possible to bypass the "safe_mode" and "open_basedir" protection mechanisms via the "ext/curl" and "ext/gd" modules.

The vulnerability has been reported in versions 4.4.0 and 5.0.5, and prior.

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

References:

Advisory:
http://www.hardened-php.net/advisory_202005.79.html
http://www.hardened-php.net/advisory_192005.78.html
http://www.hardened-php.net/advisory_182005.77.html
http://www.hardened-php.net/index.76.html
http://www.php.net/release_4_4_1.php

Other references:
http://secunia.com/advisories/17371/

Product Page:
http://www.php.net/

CVE Reference: CAN-2005-2491

❖ 16030 PHP unspecified error in calling "virtual()" on Apache 2 Vulnerability

A vulnerability has been reported in PHP, which can be exploited by malicious people to conduct cross-site scripting attacks, bypass certain security restrictions, and potentially compromise a vulnerable system.

An unspecified error in calling "virtual()" on Apache 2 can be exploited to bypass certain configuration directives (e.g. "safe_mode" and "open_basedir").

The vulnerability has been reported in versions 4.4.0 and 5.0.5, and prior.

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

References:

Advisory:
http://www.hardened-php.net/advisory_202005.79.html
http://www.hardened-php.net/advisory_192005.78.html
http://www.hardened-php.net/advisory_182005.77.html
http://www.hardened-php.net/index.76.html
http://www.php.net/release_4_4_1.php

Other references:
http://secunia.com/advisories/17371/

Product Page:
http://www.php.net/

CVE Reference: CAN-2005-2491

New Vulnerabilities found this Week

- **PHP Multiple Vulnerabilities**

  "Conduct cross-site scripting attacks, bypass certain security restrictions, and potentially compromise a vulnerable system"

  Some vulnerabilities have been reported in PHP, which can be exploited by malicious people to conduct cross-site scripting attacks, bypass certain security restrictions, and potentially compromise a vulnerable system.

  1) An error where the "GLOBALS" array is not properly protected, can be exploited to define global variables by sending a "multipart/form-data" POST request with a specially crafted file upload field, or via a script calling the PHP function "extract()" or "import_request_variables()".

  Successful exploitation may open up for vulnerabilities in various applications, but requires that "register_globals" is enabled.

  The vulnerability has been reported in versions 4.4.0 and 5.0.5, and prior.

  2) An error in the handling of an unexpected termination in the "parse_str()" PHP function, can be exploited to enable the "register_globals" directive for the current execution by e.g. triggering a memory_limit request shutdown in a script calling "parse_str()".

  The vulnerability has been reported in versions 4.4.0 and 5.0.5, and prior.

  3) Some unspecified input passed to the "phpinfo()" PHP function isn't properly sanitised before being returned to the user. This can be exploited via a script calling "phpinfo()" to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

  The vulnerability has been reported in versions 4.4.0 and 5.0.5, and prior.

  4) An integer overflow error in pcrelib may be exploited to cause a memory corruption via a script calling a PHP function using the PCRE library where the regular expression can be controlled by the attacker.

  Successful exploitation may allow execution of arbitrary code.

  5) The problem is that it is possible to bypass the "safe_mode" and "open_basedir" protection mechanisms via the "ext/curl" and "ext/gd" modules.

  6) An unspecified error in calling "virtual()" on Apache 2 can be exploited to bypass certain configuration directives (e.g. "safe_mode" and "open_basedir").

  Other bugs have also been reported where some may be security

related.

References:
http://www.hardened-php.net/advisory_202005.79.html
http://www.hardened-php.net/advisory_192005.78.html
http://www.hardened-php.net/advisory_182005.77.html
http://www.hardened-php.net/index.76.html
http://www.php.net/release_4_4_1.php

❖ **Apache Tomcat Directory Listing Denial of Service**

"Denial of Service"

David Maciejak has discovered a vulnerability in Apache Tomcat, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to the inefficient generation of directory listing for web directories that has a large number of files. By sending multiple concurrent requests for such a directory, it is possible to prevent other users from accessing the directory and causes the server to consume a large amount of CPU resources. The vulnerability affects only the directory that is being listed. Files or applications in other web directories are not affected.

Successful exploitation requires that directory listing is enabled in a directory with a large number of files.

The vulnerability has been confirmed in Tomcat version 5.5.11 and 5.5.12 on the Windows platform, and has been reported in versions 5.5.0 through 5.5.11. Other versions may also be affected.

Note: In version 5.5.12, the server will resume normal operation after a few minutes.

References:
http://secunia.com/advisories/17416/

❖ **Cisco IOS System Timers Potential Arbitrary Code Execution**

"Bypass certain security restrictions"

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

The vulnerability is caused due to an error in validating whether certain system memory has been corrupted by a heap-based buffer overflow before the internal operating system timers execute code from the affected memory area. This can potentially be exploited to execute arbitrary code in conjunction with some other heap-based buffer overflow vulnerability.

The vulnerability has been reported to affect all Cisco products that run Cisco IOS Software.

Note: The vendor has reported that the vulnerability was fixed as a result of continued research related to the demonstration of an exploit for the IPv6 vulnerability.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml

❖ **Cisco Wireless LAN Controllers Encryption Bypass Vulnerability**

"Bypass certain security restrictions"

A vulnerability has been reported in Cisco WLAN (Wireless LAN) Controllers, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to the WLAN controller accepting unencrypted traffic from end hosts even when it is configured to perform encryption. This can be exploited to send malicious traffic to a secure wireless network by spoofing the MAC address of a legitimate, already authenticated end host.

Successful exploitation requires that the access points are operating in LWAPP (Lightweight Access Point Protocol) mode, and controlled by a separate WLAN Controller.

The vulnerability has been reported in Cisco 1200, 1131, and 1240 series access points controlled by Cisco 2000 and 4400 series Airespace WLAN Controllers with software version 3.1.59.24.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20051102-lwapp.shtml

❖ **Serv-U FTP Server Potential Denial of Service Vulnerability**

"Denial of Service"

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

The vulnerability is caused due to an unspecified error and may be exploited to remotely crash the server via certain malformed packets.

NOTE: The ZLib and OpenSSL libraries have also been changed to version v1.2.3 and v0.9.8a respectively.

References:

http://www.serv-u.com/releasenotes.asp

❖ **NetBSD Update Fixes Multiple Vulnerabilities**

"Denial of Service"

Some vulnerabilities have been reported in NetBSD, which can be exploited by malicious, local users to gain escalated privileges, or by malicious users to cause a DoS (Denial of Service) and compromise a vulnerable system, or by malicious people to bypass certain security restrictions and compromise a user's system.

1) Some boundary errors exist in the telnet client. This can be exploited by malicious people to compromise a user's system.

2) Multiple vulnerabilities exist in CVS. These can be exploited by malicious users to cause a DoS (Denial of Service) and compromise a vulnerable system, or by malicious, local users to perform certain actions on a vulnerable system with escalated privileges.

3) An integer overflow error in the FreeBSD compatibility code can lead to heap corruption. This may be exploited by local users to cause a DoS and potentially to execute arbitrary code with root privileges.

4) Temporary files are being created insecurely in the "/tmp" directory by "imake" when generating pre-formatted manual pages. This can be exploited via symlink attacks to create or overwrite arbitrary files with the privileges of the user running the affected script.

5) A vulnerability exists in OpenSSL, which potentially can be exploited by malicious people to bypass certain security restrictions.

6) A security issue exists in ntpd, which can cause ntpd to run with incorrect group permissions.

7) An error exists the "ptrace()" function when checking for process privileges before attaching to a process. This can be exploited to attach to a suid process that calls "exec()". This potentially allows local privilege escalation by altering the behaviour of the process or by injecting additional syscalls.

References:
ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2005-004.txt.asc
ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2005-006.txt.asc
ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2005-008.txt.asc
ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2005-009.txt.asc

ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2005-010.txt.asc
ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2005-011.txt.asc
ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2005-013.txt.asc

❖ **Linux Kernel Potential Buffer Overflow Vulnerabilities**

Two vulnerabilities have been reported in the Linux Kernel, with an unknown impact.

1) A boundary error due to missing parameter validation in the "map_to_seg7()" function in "drivers/usb/input/map_to_7segment.h" of the Yealink driver may cause out-of-bound memory references.

2) A boundary error in "/drivers/i2c/i2c-core.c" when handling SMBus Block Write transactions may cause a buffer overflow.

References:
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=af64a5ebb817532965d18b792d6d74afecfb0bcf
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=5c50d1885981537ff3b8df6433951de6c9cb72cb
http://www.kernel.org/pub/linux/kernel/v2.6/snapshots/patch-2.6.14-git4.log

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