netVigilance

ScoutNews Team **January 21st 2005**
Issue # 3

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

The theme of stories this week is that the wheel goes round and the churn keeps going up in the digital security market:
A review finds Microsoft's Anti-Spyware worthless, a new worm pulls real-time news information from CNN to cover its intent and lure people to do what they know they shouldn't and Phishing sets a new record in volume!

Enjoy reading

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

Top Security News Stories this Week

- **Review: Microsoft Anti-Spyware Ineffective**

  Microsoft Corp. created the world's most popular operating system — one that's also heartily embraced by hackers and virus writers. And it begat the world's top Web browser, which makes it all too easy to mistakenly download and install spyware, adware and other garbage.
  You'd think the world's largest software company, which presumably knows its own Windows and Internet Explorer code, would have long ago come up with something to repair PCs possessed by malicious programs.
  Think again.
  http://story.news.yahoo.com/news?tmpl=story&ncid=1209&e=4&u=/ap/tech_test_microsoft_s_malware_scrubbers&sid=95573712
  Matthew Fordahl

- **Worm Steals CNN Headlines To Stay Timely, Fool Users**

  A new worm uses breaking news -- and a devious technique to keep itself up-to-date -- to dupe recipients into opening attachments, an anti-virus firm said Friday.
  U.K.-based security vendor Sophos said that the Crowt.a worm grabs its subject lines, message content, and attachment names from headlines culled in real-time from

CNN's Web site. The worm's subject and attachment filename constantly change to mirror the top headline on CNN.com, while the e-mail message's text is also hijacked from CNN.
http://www.techweb.com/wire/security/57702905
TechWeb News

- **Phishing Shows No Sign Of Slowing**

Phishers set another all-time record in December by creating -- and then quickly dumping -- over 1,700 bogus sites that tried to dupe users into giving up private information, the Anti-Phishing Working Group (APWG) said Friday as it released its newest report on the scam scheme.
The number of phishing Web sites -- which are created by criminals who lure consumers to them on the premise that they need to confirm or re-create lost credit card or bank account information -- in December jumped another 10 percent over November to spike at 1,707. Since August, when just 731 such sites appeared, the month-to-month increase has been a dismaying double-digit 24 percent.
http://www.techweb.com/wire/security/57702945
Gregg Keizer

New Vulnerabilities Tested in SecureScout

- **13179 Oracle Database Server - Networking component boundary error (jan-2005/DB01)**

A boundary error in the Networking component can be exploited by malicious database users to crash the database via a specially crafted connect string.

Successful exploitation requires permissions to create database links.

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

CVE Links:

Reference: http://www.oracle.com/technology/deploy/security/pdf/cpu-jan-2005_advisory.pdf & http://www.oracle.com/

- **13180 Oracle Database Server - LOB Access component unspecified error (jan-2005/DB02)**

An unspecified error in the LOB Access component can be exploited to disclose sensitive information.

Successful exploitation requires permissions to read on a database directory object.

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

CVE Links:

Reference: http://www.oracle.com/technology/deploy/security/pdf/cpu-jan-

2005_advisory.pdf & http://www.oracle.com/

- **13181 Oracle Database Server - Spatial component unspecified error (jan-2005/DB03)**

An unspecified error in the Spatial component can potentially be exploited to disclose information, manipulate data, or cause a DoS.

Successful exploitation requires execute permissions on the mdsys.md2 package.

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

CVE Links:

Reference: http://www.oracle.com/technology/deploy/security/pdf/cpu-jan-2005_advisory.pdf & http://www.oracle.com/

- **14685 Sun Java Plug-In handling of JavaScript (Remote File Checking)**

Fujitsu has reported a vulnerability in Sun Java Plug-in, which can be exploited by malicious people to bypass certain security restrictions or compromise a user's system.

An error in the Java Plug-in within the handling of JavaScript calling into Java code can e.g. be exploited by a malicious applet hosted on a web site to access and modify local files or execute local applications.

Successful exploitation requires the Microsoft Internet Explorer browser is used.

The vulnerability has been reported in SDK / JRE version 1.4.2, 1.4.1_06 and prior, all 1.4.0 releases, and 1.3.1_12 and prior for Windows.

JDK and JRE 5.0 is not affected.

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

CVE Link:

Reference: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57708-1 & http://secunia.com/advisories/13918/ & http://java.sun.com/j2se/

- **14686 Sun Java Plug-In - Applets interfering with each others (Remote File Checking)**

Fujitsu has reported a vulnerability in Sun Java Plug-in, which can be exploited by malicious people to bypass certain security restrictions or compromise a user's system.

An error in the way applets on the same web page can interfere with each other can be exploited to e.g. load files and web pages in another applet.

The vulnerability has been reported in SDK / JRE version 1.4.2_05 and prior, all 1.4.1 and 1.4.0 releases, and 1.3.1_12 and prior for Windows, Solaris and Linux.

JDK and JRE 5.0 is not affected.

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

CVE Link:

Reference: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57708-1 & http://secunia.com/advisories/13918/ & http://java.sun.com/j2se/

- **15155 PHP JPEG Image Buffer Overflow Vulnerability**

PHP is a software component used to dynamically generate Web pages.

It is reported that PHP is susceptible to a buffer overflow vulnerability in handling JPEG images. This issue is due to a failure of the application to properly bounds check user-supplied image data prior to copying it into a fixed-size memory buffer.

This vulnerability allows remote attackers to alter the proper flow of execution of the application, potentially resulting in the execution of attacker-supplied machine code in the context of the web server executing the PHP interpreter.

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

CVE Link: CAN-2004-1065

Reference: http://www.securityfocus.com/bid/11992/ & http://www.php.net/

- **15156 PHP Multiple Local And Remote Vulnerabilities**

PHP is a software component used to dynamically generate Web pages.

PHP4 and PHP5 are reported prone to multiple local and remote vulnerabilities that may lead to code execution within the context of the vulnerable process. The following specific issues are reported:

A heap-based buffer overflow is reported to affect the PHP 'pack()' function call. An attacker that has the ability to make the PHP interpreter run a malicious script may exploit this condition to execute arbitrary instructions in the context of the vulnerable process.

A heap-based memory disclosure vulnerability is reported to affect the PHP 'unpack()' function call. An attacker that has the ability to make the PHP interpreter run a malicious script may exploit this condition to reveal portions of the process heap.

PHP safe_mode_exec_dir is reported prone to an access control bypass vulnerability. A local attacker that can manipulate the directory name from which the PHP script is called, may bypass 'safe_mode_exec_dir' restrictions by placing shell metacharacters and restricted commands into the directory name of the current directory.

PHP safe_mode is reported prone to an access control bypass vulnerability. An attacker that has the ability to make the PHP interpreter run a malicious script may exploit this condition to execute commands that are otherwise restricted by PHP safe_mode.

PHP is reported prone to a 'realpath()' path truncation vulnerability. The vulnerability exists due to a lack of sanitization as to whether a path has been silently truncated by the

libc realpath() function or not. This may lead to remote file include vulnerabilities in some cases.

The PHP function 'unserialize()' is reported prone to a memory corruption vulnerability. This corruption may be leveraged by a remote attacker that has the ability to make the PHP interpreter run a malicious script to execute arbitrary code in the context of the vulnerable process.

The PHP function 'unserialize()' is also reported prone to an information disclosure vulnerability. This issue may be leveraged by a remote attacker to disclose the contents of heap memory. This may allow them to gain access to potentially sensitive information, such as database credentials.

Finally, the PHP function 'unserialize()', is reported prone to an additional vulnerability. It is reported that previous versions of this function allow a malicious programmer to set references to entries of a variable hash that have already been freed. This can lead to remote memory corruption.

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

CVE Link: CAN-2004-1018 & CAN-2004-1019 & CAN-2004-1063 & CAN-2004-1064

Reference: http://www.securityfocus.com/bid/11964/ & http://www.php.net/

- **15157 PHP Remote Arbitrary Location File Upload Vulnerability**

PHP is a software component used to dynamically generate Web pages.

PHP is vulnerable to an arbitrary location file upload vulnerability. This issue is due to a failure of the PHP application to properly sanitize user-supplied file name input.

An attacker may exploit this issue to upload files to an arbitrary location on a computer running the affected software. This may facilitate arbitrary server-side script code execution as well as other attacks.

It is reported that this issue only affects PHP versions 4.2.0 and subsequent.

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

CVE Link: CAN-2004-0959

Reference: http://www.securityfocus.com/archive/1/376865 & http://www.securityfocus.com/archive/1/375370 & http://www.php.net/ChangeLog-5.php#5.0.2

- **15158 PHP PHP_Variables Remote Memory Disclosure Vulnerability**

PHP is a software component used to dynamically generate Web pages.

A vulnerability is reported to present itself in the array parsing functions of the 'php_variables.c' PHP source file.

The vulnerability occurs when a PHP script is being used to print URI parameters or data, that are supplied by a third party, into a dynamically generated web page. It is reported

that the vulnerable function does not strip certain characters from the user supplied data, this may ultimately be harnessed to manipulate the parsing function into returning regions of process memory to the attacker.

It is reported that this issue only affects PHP versions 4.2.0 and subsequent.

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

CVE Link: CAN-2004-0958

Reference: http://www.securityfocus.com/archive/1/375294 & http://www.php.net/ChangeLog-5.php#5.0.2

- **15574 Exim 4.x - IP Address Command Line Argument Local Buffer Overflow Vulnerability**

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

A local buffer overflow vulnerability triggered by an excessively long command line argument affects Exim. This issue is due to a failure of the application to validate the length of user-supplied data prior to attempting to store it in process buffers.

An attacker may leverage this issue to execute arbitrary code with the privileges of the affected mailer application. As the application is a setuid application, it is possible that further privilege escalation may occur.

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

CVE Link: CAN-2005-0021

Reference: http://www.exim.org/mail-archives/exim-users/Week-of-Mon-20050103/msg00028.html &http://www.securityfocus.com/bid/12268/

New Vulnerabilities found this Week

- **Sun Java Plug-In Two Vulnerabilities**

"Bypass certain security restrictions"

Fujitsu has reported two vulnerabilities in Sun Java Plug-in, which can be exploited by malicious people to bypass certain security restrictions or compromise a user's system.

1) An error in the Java Plug-in within the handling of JavaScript calling into Java code can e.g. be exploited by a malicious applet hosted on a web site to access and modify local files or execute local applications.

Successful exploitation requires the Microsoft Internet Explorer browser is used.

The vulnerability has been reported in SDK / JRE version 1.4.2, 1.4.1_06 and prior, all 1.4.0 releases, and 1.3.1_12 and prior for Windows.

2) An error in the way applets on the same web page can interfere with each other can be exploited to e.g. load files and web pages in another applet.

The vulnerability has been reported in SDK / JRE version 1.4.2_05 and prior, all 1.4.1 and 1.4.0 releases, and 1.3.1_12 and prior for Windows, Solaris and Linux.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57708-1

- **KDE kpdf "Decrypt::makeFileKey2()" Buffer Overflow**

"Buffer Overflow Vulnerability"

The vendor has acknowledged a vulnerability in kpdf, which can be exploited by malicious people to compromise a user's system.

References:
http://www.kde.org/info/security/advisory-20050119-1.txt

- **Cisco IOS SCCP Control Protocol Message Denial of Service**

"Denial of Service"

SecureTest has reported a vulnerability 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 control protocol messages and can be exploited to reload a vulnerable network device via a specially crafted control protocol message sent to the SCCP (Skinny Call Control Protocol) service.

The vulnerability affects the 12.1YD, 12.2T, 12.3, and 12.3T release trains configured for Cisco IOS Telephony Service (ITS), Cisco CallManager Express (CME), or Survivable Remote Site Telephony (SRST).

References:
http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.shtml

- **Avaya Products ncompress Vulnerability**

"Arbitrary code execution"

Avaya has confirmed an old vulnerability in ncompress, which is included in various products. This can potentially be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to boundary errors within the handling of command line options in "compress" and "uncompress". This can be exploited to cause a buffer overflow by supplying e.g. a specially crafted, overly long filename.

Successful exploitation can lead to execution of arbitrary code in context of the process using the ncompress utility.

NOTE: The vendor states that ncompress is not used by any applications or network services.

The following products are affected:
* Avaya S8710/S8700/S8500/S8300 (all versions)

* Avaya Converged Communication Server (all versions)
* Avaya Network Routing (all versions)

References:
http://support.avaya.com/elmodocs2/security/ASA-2005-015_RHSA-2004-536.pdf

- **Oracle Products 23 Vulnerabilities**

"Disclose sensitive information, gain escalated privileges, conduct PL/SQL injection attacks, manipulate information, cause a DoS (Denial of Service)."

23 vulnerabilities have been reported in various Oracle products. Some have an unknown impact and others can be exploited to disclose sensitive information, gain escalated privileges, conduct PL/SQL injection attacks, manipulate information, or cause a DoS (Denial of Service).

References:
http://otn.oracle.com/deploy/security/pdf/cpu-jan-2005_advisory.pdf
http://www.nextgenss.com/advisories/oracle-02.txt
http://www.petefinnigan.com/directory_traversal.pdf
http://www.red-database-security.com/content6.html

- **Squid Username Whitespace Security Bypass Issue**

"Bypass certain security restrictions"

A security issue has been reported in Squid, which can be exploited by malicious users to bypass certain security restrictions.

The issue is caused due to some LDAP implementations ignoring leading/trailing whitespaces in usernames. This can be exploited to bypass certain ACLs based on usernames or trick some log analysis by supplying a username with a whitespace in the beginning or end during the authentication process.

The vulnerability has been reported in version 2.5 and prior.

References:
http://www.squid-cache.org/Versions/v2/2.5/bugs/#squid-2.5.STABLE7-ldap_spaces

- **Solaris/SEAM Kerberos 5 Administration Library Vulnerability**

"Heap buffer overflow"

Sun has acknowledged a vulnerability in Solaris and SEAM, which potentially can be exploited by malicious users to compromise a vulnerable system.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57712-1

- **Midnight Commander Multiple Unspecified Vulnerabilities**

"Denial of Service, escalated privileges"

Multiple vulnerabilities have been reported in Midnight Commander, where many have an unknown impact and others can be exploited to cause a DoS (Denial of Service) or potentially perform certain actions with escalated privileges.

The vulnerabilities are caused due to various types of errors including format string errors and buffer overflows.

References:
http://www.debian.org/security/2005/dsa-639

- **Apache mod_auth_radius Module Denial of Service Vulnerability**

"Denial of Service"

LSS has reported a vulnerability in the mod_auth_radius module for Apache, which potentially can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the handling of certain "RADIUS_ACCESS_CHALLENGE" RADIUS packets. This may be exploited via a man-in-the-middle attack to cause the mod_auth_radius service to crash.

The vulnerability has been reported in version 1.5.7 and prior.

References:
http://security.lss.hr/en/index.php?page=details&ID=LSS-2005-01-02

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