netVigilance

ScoutNews Team

12 December 2004
Issue #50

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

At last unified numbering of Viruses and Worms. The new CME (Common Malware Enumeration) is analogous to the CVE (Common Vulnearibility Enumeration) that we at SecureScout use everyday. Top CSO fear viruses and worms more than anything for 2005, so it is business as usual.

Enjoy reading

Top Security News Stories this Week

- ### CSOs see viruses, worms as top security challenge for '05

  Worms, viruses and Trojan horses will remain a top security concern for the coming year, according to executives attending the CSO Interchange forum in New York earlier this week.
  CSO Interchange was founded earlier this year by Howard Schmidt, eBay Inc.'s chief information security officer (CISO), and Philippe Courtot, CEO of vulnerability management provider Qualys Inc. It provides an invitation-only venue for senior IT executives to discuss security-related issues. Tuesday's meeting in New York was the second one held by the group.
  http://www.computerworld.com/securitytopics/security/story/0,10801,98195,00.html?SKC=security-98195

  Jaikumar Vijayan, Computerworld

- ### Virus names could be standardized

  US-CERT, the Computer Emergency Readiness Team within the US Department of Homeland Security, is coordinating a Common Malware Enumeration initiative among vendors, according to a letter sent to The SANS Institute.

  The letter, signed by representatives of the DHS, Symantec, Microsoft, McAfee, and Trend Micro, said the industry hopes to address "the challenges surrounding the 'Virus Name Game'," with a pilot program coming as early as January.

  http://www.cbronline.com/article_news.asp?guid=11D11704-DE5B-45BD-AF4B-45D8F44E055C

  Computer Business Review

- ### Top 10 "Most Unwanted" Spyware Named

  A security firm named the top 10 spyware threats this week, saying that the secretly-

installed software poses an "insidious" threat to consumers and corporations alike.
Webroot, which makes end-user and enterprise editions of Spy Sweeper, used its relationship with Internet service provider EarthLink to tally the most prevalent spyware, then selected the worst based on its knowledge of how each works and the damage it can cause.

"We use the P-I index," said Richard Stiennon, Webroot's vice president of threat research. "P is for prevalence, I is for insidiousness."

Each of the ten spyware programs cited by Webroot was spotted at least 50,000 times in the scans that the Boulder, Colo.-based vendor does free of charge on its own Web site, or in conjunction with EarthLink.
Full Story : http://www.techweb.com/wire/security/55301120
The Top10 List : http://www.webroot.com/company/pressreleases/20041208-spywarethreats/

Gregg Keizer, TechWeb News

- **Phishing websites grew 33% in one month**
  The number of phishing websites associated with online identity theft scams grew by 33% in November, after dropping off in September and early October, according to data compiled by the Anti-Phishing Working Group (APWG).

  The group received reports of 1,518 active phishing sites during November, up from 1,142 in October.

  Reports of phishing websites have grown by an average rate of 28% monthly since July, as scam artists broadened their efforts to lure customers of companies that do business online, according to Peter Cassidy, secretary general of the APWG.

  The APWG is an industry group of representatives from law enforcement and private sector companies, including leading internet service providers, banks and technology suppliers.
  http://www.computerweekly.com/articles/article.asp?liArticleID=135794&liFlavourID=1&sp=1

Paul Robert, IDG News Services

New Vulnerabilities Tested in SecureScout

This weeks version is 2.6.134.0

- **15444 Cyrus Imapd SASL_PATH environment variable vulnerability**
  Cyrus Imapd server is a common implementation of the IMAP4 protocol that is use mainly on unix servers.

  The libsasl and libsasl2 libraries in Cyrus-SASL 2.1.18 and earlier trusts the SASL_PATH environment variable to find all available SASL plug-ins, which allows local users to execute arbitrary code by modifying the SASL_PATH to point to malicious programs.

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

CVE Links: CAN-2004-0884

Reference: http://www.securityfocus.com/bid/11347

- ### 15445 Cyrus Imapd pre-authentication buffer overflow

  Cyrus Imapd server is a common implementation of the IMAP4 protocol that is use mainly on unix servers.

  It has been reported that Cyrus IMAPD does not sufficiently handle overly long strings. In some cases, when a user connects to the daemon, and upon negotiating the connection sends a login string of excessive length, a buffer overflow occurs. This could result in heap corruption and arbitrary words in memory being overwritten. It may be possible to exploit this issue to execute arbitrary code.

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

CVE Links: CAN-2002-1580
Reference: http://www.securityfocus.com/bid/6298

15446 Cyrus Imapd SASL library buffer overflows

Cyrus Imapd server is a common implementation of the IMAP4 protocol that is use mainly on unix servers.

Buffer overflows in Cyrus SASL library 2.1.9 and earlier allow remote attackers to cause a denial of service and possibly execute arbitrary code via long inputs during user name canonicalization, characters that need to be escaped during LDAP authentication using saslauthd, or an off-by-one error in the log writer, which does not allocate space for the null character that terminates a string.

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

CVE Links: CAN-2002-1347
Reference: http://marc.theaimsgroup.com/?l=bugtraq&m=103946297703402&w=2
http://rhn.redhat.com/errata/RHSA-2002-283.html

- ### 15447 Cyrus-SASL Imapd Syslog Format String Vulnerability

  Cyrus Imapd server is a common implementation of the IMAP4 protocol that is use mainly on unix servers.

  Cyrus SASL contains a format string vulnerability in it's internal logging function. Data that may be externally supplied is passed to syslog() as the format string argument.

  This may allow for remote attackers who can inject format specifiers into a log message to execute arbitrary code.

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

CVE Link: CAN-2001-0869

Reference: http://www.securityfocus.com/bid/3498
http://rhn.redhat.com/errata/RHSA-2001-150.html

15448 Mercury Mail Transport System Command Handling Buffer Overflows (SMTP check)

Mercury provides mail services to a single computer or a local area network.

Some vulnerabilities have been reported in Mercury Mail Transport System, which can be exploited by malicious users to compromise a vulnerable system.

The vulnerabilities are caused due to boundary errors in the handling of some commands. This can be exploited to cause a buffer overflow by supplying an overly long argument (about 512 to 1024 bytes).

The following commands are affected:
* EXAMINE
* SUBSCRIBE
* STATUS
* APPEND
* CHECK
* CLOSE
* EXPUNGE
* FETCH
* RENAME
* DELETE
* LIST
* SEARCH
* CREATE
* UNSUBSCRIBE

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

CVE Link:

Reference: http://secunia.com/advisories/13348/
http://www.pmail.com/overviews/ovw_mercwin.htm

❖ 15449 Mercury Mail Transport System Command Handling Buffer Overflows (Remote File Checking)

Mercury provides mail services to a single computer or a local area network.

Some vulnerabilities have been reported in Mercury Mail Transport System, which can be exploited by malicious users to compromise a vulnerable system.

The vulnerabilities are caused due to boundary errors in the handling of some commands. This can be exploited to cause a buffer overflow by supplying an overly long argument (about 512 to 1024 bytes).

The following commands are affected:
* EXAMINE
* SUBSCRIBE
* STATUS
* APPEND
* CHECK
* CLOSE
* EXPUNGE
* FETCH
* RENAME

* DELETE
* LIST
* SEARCH
* CREATE
* UNSUBSCRIBE

The vulnerabilities have been reported in version 4.01a. Other versions may also be affected.
Test Case Impact: **Gather Info** Vulnerability Impact: **Denial of Service** Risk: **Medium**

CVE Link:

Reference: http://secunia.com/advisories/13348/
http://www.pmail.com/overviews/ovw_mercwin.htm

❖ 15477 DMS POP3 Server Authentication Buffer Overflow Vulnerability (POP3 Check)

Reed Arvin has discovered a vulnerability in DMS POP3 Server, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error during the authentication process and can be exploited to cause a buffer overflow by supplying an overly long username or password (more than 1024 bytes).

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been confirmed in version 1.5.3.27. Other versions are reportedly also affected.
Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

CVE Link: CAN-2004-0987

Reference: http://www.digitalmapping.sk.ca/pop3srv/Update.asp

❖ 15551 Cisco VPN 3000 Concentrator Multiple Vulnerabilities (CSCdw50657)

Password Disclosure in Cisco VPN 3000 series concentrators - a family of purpose-built, remote access Virtual Private Network (VPN) platforms for data encryption and authentication.
Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

CVE Link: CAN-2002-1097

Reference:
http://www.cisco.com/en/US/products/products_security_advisory09186a00800c8154.shtml

❖ 15552 Malformed SNMP Message-Handling Vulnerabilities for Cisco Non-IOS Products (CSCdw67458)

Multiple Cisco products contain vulnerabilities in the processing of Simple Network Management Protocol (SNMP) messages.
Test Case Impact: **Gather Info** Vulnerability Impact: **Crash** Risk: **High**

CVE Link: CAN-2002-0012, CAN-2002-0013

Reference:
http://www.cisco.com/en/US/products/products_security_advisory09186a008009467b.shtml

- **15553 Cisco VPN 3000 Concentrator Multiple Vulnerabilities (CSCdx39981)**
  When using a VPN client it is possible to cause the Cisco VPN 3000 series concentrator to reload by responding with a very large string for the username prompt.
  The Cisco VPN 3000 series concentrators are a family of purpose-built, remote access Virtual Private Network (VPN) platforms for data encryption and authentication.

Test Case Impact: **Gather Info** Vulnerability Impact: **Denial of Service** Risk: **High**

CVE Link: CAN-2002-1095

Reference:
http://www.cisco.com/en/US/products/products_security_advisory09186a00800c8154.shtml

New Vulnerabilities found this Week

- **Linux Kernel "sys32_ni_syscall" and "sys32_vm86_warning" Buffer Overflows**
  “Buffer overflows”

  Jeremy Fitzhardinge has reported some potential vulnerabilities with an unknown impact in the Linux Kernel.

  The vulnerabilities are caused due to boundary errors within the "sys32_ni_syscall()" and "sys32_vm86_warning()" functions and can be exploited to cause buffer overflows.

  The attack vectors and impact are currently unknown.

  References: http://www.ussg.iu.edu/hypermail/linux/kernel/0411.3/1467.html

- **Squid Malformed Host Name Error Message Information Leakage**
  “Gain knowledge of potentially sensitive information”

  Artur Szostak has reported a vulnerability in Squid, which can be exploited by malicious people to gain knowledge of potentially sensitive information.

  The vulnerability is caused due to an error when returning error messages in response to malformed host names. This may in certain circumstances leak random information about e.g. other requests in the error messages.

  The vulnerability has been reported in Squid-2.5 on all platforms.

  References: http://www.squid-cache.org/bugs/show_bug.cgi?id=1143

- ### rootsh Escape Sequences Logging Security Bypass

  “Bypass the logging functionality”

  A security issue has been reported in rootsh, which can be exploited by malicious, local users to bypass the logging functionality.

  The problem is caused due to an input validation error when handling certain xterm escape sequences. This can be exploited to generate empty syslog messages, allowing users to hide their actions in a syslog-only environment.

- ### Microsoft Internet Explorer "sysimage:" Local File Detection Weakness

  “Detect the presence of local files”

  Gregory R. Panakkal has discovered a weakness in Internet Explorer, which can be exploited by malicious people to detect the presence of local files.

  The "sysimage:" URI handler is used for referencing embedded icons in executable files. The problem is that a website in the "Internet" zone can reference the URI handler in an image tag. This can be exploited to determine the presence of local programs using the "onerror" and "onload" events.

  The weakness has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP1.

- ### Microsoft Browser Client Context Tool Three Vulnerabilities

  “Cross-site scripting attacks”

  Nicolas Gregoire has reported some vulnerabilities in Microsoft Browser Client Context Tool (W3Who.dll), which can be exploited by malicious people to conduct cross-site scripting attacks or potentially compromise a vulnerable system.

  1) Invalid input passed to the ISAPI extension is not properly sanitised before being returned to users in error messages. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable web site.

  Example:
  http://[host]/scripts/w3who.dll?bogus=[code]

  2) Input passed in HTTP headers is not properly sanitised before being displayed. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable web site.

  3) A boundary error within the processing of parameters can be exploited to cause a buffer overflow by passing an overly long parameter.

Example:
http://[host]/scripts/w3who.dll?AAAAAAAAA...[519 to 12571]....AAAAAAAAAAAAAA

References: http://www.exaprobe.com/labs/advisories/esa-2004-1206.html

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