netVigilance

ScoutNews Team

3 December 2004
Issue #49

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review
Top Security News Stories this Week
New Test Cases Tested in SecureScout
New Vulnerabilities this Week

This Week in Review

Lycos Europe N.V has turned vigilante in the fight against SPAM, recruiting users all over the world to participate in a Distributed Denial of Service (DDOS) attack against web-sites using SPAM as advertising tool. Spam is the black plague of the internet with 70% of all email being spam, but netVigilance thinks that breaking the law in retribution against spammers is not the answer. There are many good initiatives out there to end spam once and for all. We just need all to start implement them.

Enjoy reading

Top Security News Stories this Week

- **Lycos Europe confronts strong resistance in spam war**
  In declaring war on spammers, Lycos Europe N.V. has stirred a formidable enemy.
  The online community/portal company's offensive against spammers began this week, when it started distributing a screensaver that conducts a denial-of-service attack against sites that market products via spam.
  The weaponry has had an impact, decreasing the response time of some of the targeted sites by as much as 85 percent, Lycos Europe said.
  The enemy, however, has apparently rallied its troops in a counteroffensive.
  http://www.itnews.com.au/msoft_storycontent.asp?ID=9&Art_ID=22745

Antone Gonsalves, TechWeb

- **Security guru being pestered by the FBI for logs...**

  The creator of the famous hacking tool Nmap is being hounded by the FBI for copies of web server log data from his Web site Insecure.org.

  Fyodor, as he is known, is a well known figure in the security world, specifically for his work with Nmap. In his blog, Fyodor said that the authorities were asking him for details but failing to give reasons of what they were up to.
  http://software.silicon.com/security/0,39024655,39126180,00.htm

Dan Ilett, silicon.com

- **HP wants to 'Throttle' viruses with software**
  HP aims to slow the progress of viruses...

HP plans to give customers a new weapon against viruses: software that crimps their spread.

Early next year, the computer maker will begin selling software designed to slow the spread of viruses from its ProLiant servers and ProCurve networking equipment, an HP executive said on Tuesday. A version for HP's personal computers is planned for later release.

http://software.silicon.com/security/0,39024655,39126217,00.htm

Stephen Shankland, CNET News

- **New security standards to strengthen SCADA**

  Industrial control systems seen as vulnerable to Internet threats

  The security of critical-infrastructure processes, long festering as a thorny issue in securing everything from food and water to energy and transportation, will be getting a boost from proposed standards for industrial controls.

  http://www.computerworld.com/securitytopics/security/holes/story/0,10801,97606,00.html?SKC=holes-97606

Mark Willoughby, Computerworld

New Vulnerabilities Tested in SecureScout

This weeks version is 2.6.133.0

- **14669 Cumulative Security Update for Internet Explorer (MS04-040/889293) (Remote File Checking)**

  A vulnerability exists in Internet Explorer that could allow remote code execution on an affected system.

  If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability 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 Links: CAN-2004-1050

Reference: http://www.microsoft.com/technet/security/bulletin/ms04-040.mspx

- **15436 Cyrus Imapd 2.2.x IMAPMAGICPLUS preauthentification overflow**

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

  When the option imapmagicplus is activated on a server the PROXY and LOGIN commands suffer a standard stack overflow, because the username is not checked against a maximum length when it is copied into a temporary stack buffer. This bug is especially dangerous because it can be triggered before any kind of authentification took place.

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

CVE Links: CAN-2004-1011

Reference: http://security.e-matters.de/advisories/152004.html

- **15441 Cyrus Imapd PARTIAL command out of bounds memory corruption**

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

  An input validation error within the argument parser for the "PARTIAL" command can be exploited to reference memory outside an allocated buffer.

  Combined with another error, successful exploitation allows overwriting a single byte, which may allow execution of arbitrary code.

  This vulnerability has been reported in version 2.2.6 and prior.

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

CVE Links: CAN-2004-1012

Reference: http://security.e-matters.de/advisories/152004.html

- **15442 Cyrus Imapd FETCH command out of bounds memory corruption**

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

  An input validation error within the argument handler for the "FETCH" command can be exploited to reference memory outside an allocated buffer.

  Combined with another error, successful exploitation allows overwriting a single byte, which may allow execution of arbitrary code.

  This vulnerability has been reported in version 2.2.8 and prior.

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

CVE Link: CAN-2004-1013

Reference: http://security.e-matters.de/advisories/152004.html

- **15443 Cyrus Imapd 2.2.x APPEND command uses undefined programming construct**

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

  The handler for the "APPEND" command uses an undefined programming construct, which potentially could result in an attacker-supplied pointer being freed.

  Successful exploitation may potentially allow execution of arbitrary code.

  This vulnerability has been reported in versions 2.2.7 and 2.2.8.

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

CVE Link: CAN-2004-1015

Reference: http://security.e-matters.de/advisories/152004.html

❖ 15546 Cisco IOS ARP Table Overwrite Vulnerability (CSCdu81936)

It is possible to send an Address Resolution Protocol (ARP) packet on a local broadcast interface (for example, Ethernet, cable, Token Ring, FDDI) which could cause a router or switch running specific versions of Cisco IOS® Software Release to stop sending and receiving ARP packets on the local router interface.

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

CVE Link: CVE-2001-0895

Reference:
http://www.cisco.com/en/US/products/products_security_advisory09186a00800b113c.shtml

❖ 15547 Cisco VPN 3000 Concentrator Multiple Vulnerabilities (CSCdu82823)

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: **Crash** Risk: **High**

CVE Link: CVE-2001-0427

Reference: http://www.cisco.com/warp/public/707/vpn3k-multiple-vuln-pub.shtml

❖ 15548 A Vulnerability in IOS Firewall Feature Set (CSCdv48261)

The IOS Firewall Feature set, also known as Cisco Secure Integrated Software, also known as Context Based Access Control (CBAC), and introduced in IOS version 11.2P, has a vulnerability that permits traffic normally expected to be denied by the dynamic access control lists.

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

CVE Link: CVE-2001-0929

Reference:
http://www.cisco.com/en/US/products/products_security_advisory09186a00800941ee.shtml

❖ 15549 Cisco VPN 3000 Concentrator Multiple Vulnerabilities (CSCdv66718)

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: **Crash** Risk: **High**

CVE Link: CAN-2002-1092

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

- **15550 Cisco CatOS Telnet Buffer Vulnerability (CSCdw19195)**
  Some Cisco Catalyst switches, running certain CatOS based software releases, have a vulnerability wherein a buffer overflow in the Telnet option handling can cause the Telnet daemon to crash and result in a switch reload.

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

CVE Link: CVE-2001-0554

Reference:
http://www.cisco.com/en/US/products/products_security_advisory09186a0080094b65.shtml

New Vulnerabilities found this Week

- **Sun Solaris Netscape PNG Image Handling Vulnerabilities**
  "Denial of Service"

  Sun has acknowledged some vulnerabilities in the Netscape browser for Solaris, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a user's system.

  References:
  http://sunsolve.sun.com/search/document.do?assetkey=1-26-57683-1

- **Sun Solaris ping Utility Privilege Escalation Vulnerability**
  "Buffer overflow, execution of arbitrary code with escalated privileges"

  A vulnerability has been reported in Sun Solaris, which can be exploited by malicious, local users to gain escalated privileges.

  The vulnerability is caused due to an unspecified boundary error within the ping utility and can be exploited to cause a buffer overflow.

  Successful exploitation allows execution of arbitrary code with escalated privileges.

  References:
  http://sunsolve.sun.com/search/document.do?assetkey=1-26-57675-1

- **WS_FTP Server FTP Commands Buffer Overflow Vulnerabilities**
  "Execution of arbitrary code"

Reed Arvin has discovered some vulnerabilities in WS_FTP Server, which can be exploited by malicious users to compromise a vulnerable system.

The vulnerabilities are caused due to boundary errors within the handling of the "SITE", "XMKD", "MKD", and "RNFR" commands. This can be exploited to cause a buffer overflow by supplying an overly long argument (about 768 bytes).

Successful exploitation allows execution of arbitrary code.

The vulnerabilities have been confirmed in version 5.03. Other versions may also be affected.

References:
http://secunia.com/advisories/13334/

- **Orbz Password Field Buffer Overflow Vulnerability**
  “Execution of arbitrary code”

  Luigi Auriemma has reported a vulnerability in Orbz, which potentially can be exploited by malicious people to compromise a vulnerable system.

  The vulnerability is caused due to a boundary error when handling join requests. This can be exploited to cause a buffer overflow by supplying an overly long password.

  Successful exploitation may allow execution of arbitrary code.

  The vulnerability has been reported in version 2.10 and prior.

  References:
  http://aluigi.altervista.org/adv/orbzbof-adv.txt

- **Microsoft Windows WINS Replication Packet Handling Vulnerability**
  “Execution of arbitrary code”

  Nicolas Waisman has reported a vulnerability in Microsoft Windows, which can be exploited by malicious people to compromise a vulnerable system.

  The vulnerability is caused due to an error within WINS (Windows Internet Name Service) during the handling of replication packets. This can be exploited to write 16 bytes to an arbitrary memory location by sending a specially crafted WINS replication packet to a vulnerable server.

  Successful exploitation allows execution of arbitrary code.

  The vulnerability has been reported in Windows 2000 SP2 through SP4. However, other versions are reportedly also believed to be affected.

  References:

http://www.immunitysec.com/downloads/instantanea.pdf
http://www.kb.cert.org/vuls/id/145134

- **Internet Explorer HTML Elements Buffer Overflow Vulnerability**
  "Execution of arbitrary code"

  A vulnerability has been reported in Internet Explorer, which 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 certain attributes in the <IFRAME> and <FRAME> HTML tags. This can be exploited to cause a buffer overflow via a malicious HTML document containing overly long strings in e.g. the "SRC" and "NAME" attributes of the <IFRAME> tag.

  Successful exploitation allows execution of arbitrary code.

  The vulnerability has been confirmed in the following versions:
  * Internet Explorer 6.0 on Windows XP SP1 (fully patched).
  * Internet Explorer 6.0 on Windows 2000 (fully patched).

  References:
  http://www.microsoft.com/technet/security/bulletin/ms04-040.mspx
  http://www.kb.cert.org/vuls/id/842160

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