netVigilance

ScoutNews Team **2 April 2004**
Issue #14

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Yet another week that kept us all on our toes!
The world's largest infrastructure company – Cisco is now targeted with an intelligent hackers tool kit. Microsoft and some Linux versions are talking about their improvements within Security and ISS is slammed because they expect users to pay for their product upgrades – We all expect everything for free now and even harass companies that try to get paid for their work that offers value – where will this end?
The worms continue to flow over us and VA testing is more important than ever.
Enjoy the reading.

Top Security News Stories this Week

- **ISS slammed for 'selling' security patches**

ISS's security products were last week attacked by the Witty worm but the company is refusing to provide patches to customers who do not have a valid maintenance contract. Security vendor ISS has been slammed for only providing security patches to customers who have purchased a maintenance agreement from the company. Last week, this left about 12,000 computers vulnerable to the Witty worm, which has proved one of the most destructive worms to be released for a number of years. The Witty worm started to spread less than two days after a flaw in Internet Security Systems (ISS) RealSecure and BlackIce products was disclosed. The worm is unusual in that it is one of the first worms in recent years to have a physically destructive payload -- it was designed to regularly write small amounts of data to random places on an infected machine's hard drive, which causes loss of data and eventually crashes the computer.
http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?database=JanEE%2edb&command=viewone&id=8&op=t
Munir Kotadia for ZDNet UK

- **Gates e-mails security brain dump to customers**

Offers laundry list of initiatives under way at Microsoft

Microsoft Corp. Chairman and Chief Software Architect Bill Gates reached out to his company's customers on Wednesday in an e-mail that detailed the company's work to secure its software products. In the message, Gates called computer security "as big and important a challenge as any our industry has ever tackled," and said Microsoft is making "significant progress on the security front." The mammoth, 3,500 word e-mail was sent to customers who subscribed to receive executive e-mail and was titled "A Microsoft Progress Report: Security." In it, Gates presents a laundry list of security initiatives at the Redmond, Washington, company.

Among the developments Gates cites as evidence of progress on the security front are features in the forthcoming Windows XP Service Pack 2 and Windows Server 2003 Service Pack 1 and more…

http://www.infoworld.com/article/04/03/31/HNgatessecurity_1.html?source=rss&url=http://www.infoworld.com/article/04/03/31/HNgatessecurity_1.html
By Paul Roberts, IDG News Service

- **Cisco warns of new hacking toolkit**

  Public release of computer code exploits security vulnerabilities in Cisco products.

Cisco Systems Inc. during the weekend warned customers about the public release of computer code that exploits multiple security vulnerabilities in Cisco products.
Using exploits for nine software vulnerabilities, the program could allow malicious hackers to compromise Cisco's popular Catalyst switches or a wide variety of machines running versions of the company's Internetwork Operating System (IOS), Cisco said on Saturday.

Called the "Cisco Global Exploiter," the program appears to give users a menu of choices, depending on the system they are trying to crack. For example, the "Cisco 677/678 Telnet Buffer Overflow Vulnerability," or "Cisco Catalyst 3500 XL Remote Arbitrary Command Vulnerability," according to the Web site, www.k-otik.com.

http://www.infoworld.com/article/04/03/29/HNhackingtoolkit_1.html?source=rss&url=http://www.infoworld.com/article/04/03/29/HNhackingtoolkit_1.html
By Paul Roberts, IDG News Service

- **Security Enhanced Linux**

Operating system security is (or at least should be) of critical importance to us all. However, the varying levels of security required differ for each systems administrator.

For those who seek enhanced, tightened security control over their Linux systems, SELinux may be the answer. Standing for Security-Enhanced Linux, it is a result of research projects from the NSA (National Security Agency) in the US and focuses on mandatory access controls which offers powerful controls over users and devices as well as applications and services.

http://www.sitepoint.com/blog-post-view.php?id=161027&ct=1

by Blane Warrene

- **Windows Vs. Linux Security: Depends On Who**

A new Forrester Research study says the question of which operating system is more secure depends greatly on what aspects of security companies see as most important. Although the knee-jerk response from IT professionals is that Linux is more secure than Windows, the real answer is a lot more complex, according to a recently-released report from Forrester Research.

"When asked about the security of popular operating systems like Linux and Windows, many IT professionals have a reflexive reaction: Linux is relatively secure; Windows isn't," Laura Koetzle, a senior analyst with Forrester said Wednesday.

http://www.informationweek.com/story/showArticle.jhtml?articleID=18700097
By Gregg Keizer, TechWeb News

- **Software industry makes room for government**

Companies acknowledge possible need for new security rules

WASHINGTON (AP) -- In a surprise shift, leading software companies acknowledge in a report to the Bush administration that the government might need to force the U.S. technology industry to improve the security of America's computer networks.

The companies, including Microsoft Corp. and Computer Associates International Inc., said the Homeland Security Department "should examine whether tailored government action is necessary" to compel improvements in the design of computer software.

http://www.cnn.com/2004/TECH/internet/04/01/cybersecurity.ap/index.html
CNN.com

New Vulnerabilities Tested in SecureScout

- **14206 No User Profile Required Vulnerability**

  User profiles can be used to restrict user access.
  It was found that no user profile is required for the user.

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

CVE Link: No CVE link available

- **14419 W32/Netsky.p Worm**

  This virus spreads via email, mapped drives and peer to peer . It sends itself to addresses found on the victim's machine.

  ** Installation **

  The worm copies itself into %WinDir% (eg. C:WINDOWS) folder using the filename FVProtect.exe

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

  CVE Link: No CVE link available
  References:
  http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101119

- **14420 W32/Polybot.l!irc Worm (phatbot/Agobot.FO) (Registry Check)**

  This variant belongs to a family of IRC bots based on W32/Gaobot.worm group. The worm bears the following characteristics:

  * Spreads through shares
  * Stealthy and hides itself in memory. The file is deleted.
  * Connects to IRC servers to perform various functions
  * Terminates security services
  * Carries out Denial of Service attack
  * Modifies hosts file on infected system
  * May spread through MS03-026 vulnerability

  Test Case Impact: **Gather Info** Vulnerability Impact: **Gain Root** Risk: **Medium**

  CVE Link: No CVE link available
  References: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101100
  http://www.f-secure.com/v-descs/agobot_fo.shtml

- **17643 Microsoft IIS WebDAV Buffer Overflow (MS03-007/Q815021) (DOS)**

  IIS server is Microsoft's HTTP server for various platforms.
  Version 5.0 of this server is vulnerable to a buffer overflow when using the WebDAV feature. The problem lies within the ntdll.dll which allows for remote code execution.
  Note that WebDAV is enabled by default.
  Windows NT 4 and Windows XP versions are not vulnerable.

  Test Case Impact: **DoS** Vulnerability Impact: **Gain Root** Risk: **High**

  CVE Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0109

  Microsoft Security Bulletin: http://www.microsoft.com/technet/security/bulletin/MS03-007.asp

CERT advisory: http://www.cert.org/advisories/CA-2003-09.html
NTBugTraq NTDLL Attack FAQ: http://www.ntbugtraq.com/ntdll.asp
How to disable WebDAV: http://support.microsoft.com/default.aspx?scid=kb;EN-US;241520
How to protect you from the vulnerability:http://support.microsoft.com/default.aspx?scid=kb;en-us;816930
BID: http://www.securityfocus.com/bid/7116
SANS Top 20 Internet Information Services (IIS): http://www.sans.org/top20/#W1

- **19019 Hijack CrackedEarth**

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: No CVE link available
URL: http://www.pestpatrol.com/PestInfo/c/crackedearth.asp

- **19020 Hijack CustomToolbar**

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: No CVE link available
URL: http://www.pestpatrol.com/PestInfo/c/customtoolbar.asp

- **19021 Hijack CWS (CoolWebSearch)**

Hijacker that runs a Java applet. Requires older or unpatched version of Microsoft Internet Explorer. Some variants (eg., CWS.Vrape) will redirect to adult sites or invoke dialers.

ALIAS: Adult Search bar (CWS.CameUp), Blackbox Trojan, Cool Web Search, Exploit-ByteVerify, Java/Shinwow.F.Blackbox.Trojan, JS.Exception.Exploit, PopMonster, Trojan.Bootconf, Trojan.Qhosts.A, Trojan.Qhosts.B, Trojan.Win32.Krepper.f, Trojan.Win32.Madise.a, Trojan.Win32.StartPage.bn, Verify

Exploit: Most exploits IE to allow a .css (Cascading Style Sheet) to run Javascript. The exploit only works if the system has the "ByteCode Verifier" vulnerability. A patch for this vulnerability has been available since April 9, 2003.
Some of the .Aff variants exploit the "Microsoft VM ActiveX Component" vulnerability.:

Microsoft Virtual Machine (VM) in Internet Explorer 4.x and 5.x allows an unsigned applet to create and use ActiveX controls, which allows a remote attacker to bypass Internet Explorer's security settings and execute arbitrary commands via a malicious web page or email.

Advertising: Yes. In CWS.DataNotary and CWS.BootConf, the script embedded in this style sheet may open porn pop-ups if it thinks the page being viewed is porn-related. CWS.MSSPI will pop up ad links in a window after every few pages viewed on a targeted search engine.

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: No CVE link available

Original Advisory: http://www.pestpatrol.com/pestinfo/c/cws.asp

New Vulnerabilities this Week

OpenPKG Security Advisory: squid (OpenPKG-SA-2004.008)
« Squid bypass certain access controls »

According to a security advisory from the vendor, a vulnerability exists in the URL unescaping logic of the Squid Web Proxy Cache. This bug could allow an attacker to bypass certain access controls by inserting a NUL character into decoded URLs. The Common Vulnerabilities and Exposures (CVE) project assigned the id CAN-2004-0189 to the problem.
For more information, see http://securityfocus.com/advisories/6508 & http://www.openpkg.org/security.html
Source: Security Focus

Mandrakelinux Security Update Advisory: ethereal
« thirteen buffer overflows & run arbitrary code »

A number of serious issues have been discovered in versions of Ethereal prior to 0.10.2. Stefan Esser discovered thirteen buffer overflows in the NetFlow, IGAP, EIGRP, PGM, IrDA, BGP, ISUP, and TCAP dissectors. Jonathan Heusser discovered that a carefully-crafted RADIUS packet could cause Ethereal to crash. It was also found that a zero-length Presentation protocol selector could make Ethereal crash. Finally, a corrupt color filter file could cause a segmentation fault. It is possible, through the exploitation of some of these vulnerabilities, to cause Ethereal to crash or run arbitrary code by injecting a malicious, malformed packet onto the wire, by convincing someone to read a malformed packet trace file, or by creating a malformed color filter file.
For more information, see http://securityfocus.com/advisories/6499 & http://www.ethereal.com/appnotes/enpa-sa-00013.html
Source: Security Focus

Gentoo Linux Security Advisory: MPlayer
« Remote buffer overflow in MPlayer »

A vulnerability exists in the MPlayer HTTP parser which may allow an attacker to craft a special HTTP header ("Location:") which will trick MPlayer into executing arbitrary code on the user's computer. An attacker without privileges may exploit this vulnerability remotely, allowing arbitrary code to be executed in order to gain unauthorized access.
For more information, see http://securityfocus.com/advisories/6498 & http://www.mplayerhq.hu/homepage/design6/news.html
Source: Security Focus

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