netVigilance

ScoutNews Team **18 January 2004**
Issue #3

Weekly SecureScout News by netVigilance

Table of Contents

Top Security News Stories this Week

❖ 'Serial ID thieves' banned from auction sites

A US Federal Court last week imposed an order prohibiting two alleged ID fraudsters from taking part in Internet auctions. The duo was also ordered to pay more than $93,000 in compensation to consumers at the end of a civil case brought by US consumer watchdogs.
http://www.theregister.co.uk/content/55/34815.html
By John Leyden – The Register, Jan 12th 2004

❖ P2P file swapping back on the increase

As you were, then. Hot on the heels of tentative claims of victory over file-swappers by the music industry, the number of dangerous, music downloading criminals started climbing again in the US. Illegal music downloader numbers had been falling for six months, according to NPD Group, but a survey by the outfit reports that they climbed six per cent in October and seven per cent in November.

http://www.theregister.co.uk/content/6/34936.html
By John Lettice – The Register, Jan 16th 2004

❖ Researcher for whom exploit code means freedom of speech

Georgi Guninski is a man who is respected on vulnerability mailing lists. The Bulgarian security expert - and this is one instance when the word can be safely used - has spread himself wide when it comes to security but all of his vulnerability posts merit attention.

From kernel bugs to browser holes, Guninski has found them all. His advisories are terse and to the point but cause a predictable degree of consternation when they are put out. His own favourite discovery is a race condition in the OpenBSD kernel.

http://www.linuxsecurity.com/articles/general_article-8770.html
By David Isecke – SMH.com, Jan 16th 2004

❖ Who's Patching Open Source? - Part 2

In one of the great ironies of the software industry, Covalent's management software -- though known for open-source management -- is a proprietary product. Unlike most of the programs it manages, the CAM software code is not transparent or changeable by those who use it.

http://cio-today.newsfactor.com/story.xhtml?story_title=Who_s_Patching_Open_Source____Part__&story_id=22998&category=netsecurity
By James Maguire – Enterprise LinuxIT, Jan 15th 2004

New Vulnerabilities Tested for in SecureScout

- **14385 Windows NT automatically logs in an administrator**

  Windows systems can automatically log in an administrator and therefore any user who has physical access to the machine will be able to use the console as administrator without entering any password. This is a very high security risk and it is recommended that you deactivate the use of Auto Admin Logon.

  Test Case Impact: **Gather Info;** Vulnerability Impact: **Gain Root;** Risk: **High**

  CVE Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0549

- **14386 Floppy Allocation Vulnerability**

  A Windows NT system does not restrict access to removable media drives such as a floppy disk drive. The floppy disk is available to all users on the system including network users. For best security practice, the floppy disk should only be available to the user who is logged on at the console.

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

  CVE Links: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0594

- **14387 Buffer Overrun in MDAC Function Could Allow Code Execution (MS04-003/832483)**

Microsoft Data Access Components (MDAC) is a collection of components that provides the underlying functionality for a number of database operations, such as connecting to remote databases and returning data to a client. When a client system on a network tries to see a list of computers that are running SQL Server and that reside on the network, it sends a broadcast request to all the devices that are on the network. Because of vulnerability in a specific MDAC component, an attacker could respond to this request with a specially-crafted packet that could cause a buffer overflow. An attacker who successfully exploited this vulnerability could gain the same level of privileges over the system as the program that initiated the broadcast request. The actions an attacker could carry out would be dependent on the permissions under which the program using MDAC ran. If the program ran with limited privileges, an attacker would be limited accordingly; however, if the program ran under the local system context, the attacker would have the same level of permissions.

Test Case Impact: **Gather Info;** Vulnerability Impact: **Gain Root;** Risk: **High**

CVE Links: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0903
Initial Advisory: http://www.microsoft.com/technet/security/bulletin/ms04-003.asp

- **14388 Vulnerability in Exchange Server 2003 Could Lead to Privilege Escalation (MS04-002/832759)**

Vulnerability exists in the way that Hypertext Transfer Protocol
(HTTP) connections are reused when NTLM authentication is used between front-end Exchange 2003 servers providing OWA access and, when running Outlook Web Access (OWA) on Windows 2000 and Windows Server 2003, and when using back-end Exchange 2003 servers that are running Windows Server 2003. Users who access their mailboxes through an Exchange 2003 front-end server and Outlook Web Access might get connected to another user's mailbox if that other mailbox is (1) hosted on the same back-end mailbox server and (2) if that mailbox has been recently accessed by its owner. Attackers seeking to exploit this vulnerability could not predict which mailbox they might become connected to. The vulnerability causes random and unreliable access to mailboxes and is specifically limited to mailboxes that have recently been accessed through OWA. By default, Kerberos authentication is used as the HTTP authentication method between Exchange Server 2003 front-end and back-end Exchange servers. This behavior manifests itself only in deployments where OWA is used in an Exchange front-end/back-end server configuration and Kerberos has been disabled as an authentication method for OWA communication between the front-end and back-end Exchange servers. This vulnerability is exposed if the Web site that is running the Exchange Server 2003 programs on the Exchange back-end server has been configured not to negotiate Kerberos authentication, causing OWA to fall back to using NTLM authentication. The only known way that this vulnerability can be exposed is by a change in the default configuration of Internet Information Services 6.0 on the Exchange back-end server. This vulnerability cannot be exposed by a routine fallback to NTLM because of a problem with Kerberos authentication. This configuration change may occur when Microsoft Windows SharePoint Services (WSS) 2.0 is installed on a Windows Server 2003 server that also functions as an Exchange Server 2003 back-end.

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

CVE Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0904
Microsoft Link: http://www.microsoft.com/technet/security/bulletin/ms04-002.asp

- **17861 Coreutils LS Width Argument Integer Overflow Vulnerability trigger a Freeze on wu-ftp**

Coreutils 'ls' has been reported prone to an integer overflow vulnerability. The issue reportedly presents itself when handling width and column display command line arguments. It has been reported that excessive values passed as a width argument to 'ls' may cause an internal integer value to be misrepresented. Further arithmetic performed based off this misrepresented value may have unintentional results. Additionally this vulnerability may be exploited in wu-ftp server that implements and invokes the vulnerable 'ls' utility to trigger a freeze or in certain conditions a denial of service.

Test Case Impact: **Denial of Service;** Vulnerability Impact: **Denial of Service;** Risk: **High**

CVE Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0854
Original disclosure: http://lists.netsys.com/pipermail/full-disclosure/2003-October/012548.html
Conectiva: http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000768;
http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000771;
Redhat: http://www.redhat.com/support/errata/RHSA-2003-309.html;
http://www.redhat.com/support/errata/RHSA-2003-310.html

- **15862 wu-ftpd globbing buffer overflow vulnerability**

Vulnerability in wu-ftpd up to version 2.6.1, which is unrelated to the ftpglob bug described in CAN-2001-0550. The glob function overwrites buffer bounds while matching open and closed brackets. Due to a missing \ 0 at the end of the buffer a later call to a function that frees allocated memory will feed free (3) with user defined data. This bug could be exploited depending on the implementation of the dynamic allocateable memory API (malloc (3), free (3)) in the libc library. Linux and other system are exploitable.

Test Case Impact: **Attack;** Vulnerability Impact: **Attack/Gain Root;** Risk: **High**

CVE Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0935
Original disclosure: http://sourceforge.net/forum/forum.php?forum_id=308015
Conectiva: http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000778

- **17863 wu-ftpd SITE NEWER vulnerability FTP**

Wu-ftpd SITE NEWER command consumes excessive amounts of memory that could lead to a denial of service attack. The SITE NEWER command is a feature specific to wu-ftpd designed to allow mirroring software to identify all files newer than a supplied date. Local and remote attackers could use the SITE NEWER command to perform a denial of service attack and execute arbitrary code with ftp user privileges, usually root.

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

CVE Link: No CVE link available
BID: http://www.securityfocus.com/bid/4257
Product Page: http://www.surfcontrol.com/

New Vulnerabilities this Week

Vulnerability Issues in Implementations of the H.323 Protocol
During 2002 the University of Oulu Security Programming Group (OUSPG) discovered a number of implementation specific vulnerabilities in the Simple Network Management Protocol (SNMP). Subsequent to this discovery, NISCC has performed and commissioned further work on identifying implementation specific vulnerabilities in related protocols that are critical to the UK Critical National Infrastructure. One of these protocols is H.225 which is part of the H.323 family and commonly implemented as a component of multimedia applications such as Voice Over IP.

OUSPG has produced a test suite for H.225 and employed it to validate their findings against a number of products from different vendors. The test results have been confirmed by testing performed by NISCC and the affected vendors contacted with the test results. These vendors' product lines cover a great deal of the existing critical information infrastructure worldwide and have therefore been addressed as a priority. However, NISCC has subsequently contacted other vendors whose products employ H.323 and provided them with tools with which to test these implementations.
For more information, see http://www.uniras.gov.uk/vuls/2004/006489/h323.htm
Source: NISCC

Security flaws force Linux kernel upgrade
Open-source developers released a new version of the Linux kernel Monday in a move aimed at quickly fixing several bugs--among them two serious security flaws.

The 2.4.24 upgrade to the Linux kernel comes a month after the release of the previous version of the core system software and only includes patches for six software issues, including the two flaws.

The release is intended to prompt users to upgrade quickly, said Marcelo Tosatti, the maintainer of the 2.4 kernel series and a Linux developer for data center management company Cyclades.

"These security issues need to be fixed as soon as possible," Tosatti told CNET News.com in an interview Monday. As maintainer, Tosatti decides what changes can be made to the kernel and when to release new versions of the core system software for Linux.

For more information, see http://www.business-standard.com/ice/story.asp?Menu=119&story=31655
By Robert Lemos

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.