netVigilance

ScoutNews Team **12 July 2004**
Issue #28

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

The Global Information Security Survey, which questioned 7,000 business technology and security professionals in 40 countries, was released last week. It has created a lot of good debate;

"Businesses hit by viruses and hackers" - reads like an advertisement for computer security firms - or a condemnation of their products.

The Global Information Security Survey says that computer hackers and viruses attacked almost all businesses world wide.
Researchers found many businesses were not following best practice security advice, but that most intended to spend more money in an effort to combat the problem.

IT security is a cost – how should you view it? And who is responsible? Two of the stories we link to here discuss these issues.

Microsoft has lost market share in the browser market segment for the first time in a long time. This is believed to be rooted in security concerns. However the loss is from 95 to 94 percent, so obviously we have 94 percent of the browser market not concerned about security if we take the numbers as proof – or disregard the functionality user's value over security.

And… Once again we have the Windows versus Linux debate.

Enjoy reading

Top Security News Stories this Week

- **IE suffers security concerns, loses market share**

Internet Explorer last month saw its market share drop for the first time this century, according to WebSideStory. Total market share fell by 1 per cent in June. "It's the first time that we've seen a sustained trend downward for (Microsoft)" said Geoff Johnston, an analyst with WebSideStory. "We have a very steady trend. It's been about a month, and every day we have a steady incremental change."
Internet Explorer has held more than 95 per cent of the browser market since June 2002, and

until June had remained steady with about 95.7 per cent of the browser market, according to WebSideStory's measurements. Over the last month, however, its market share has slowly dropped from 95.73 per cent on June 4 to 94.73 per cent on July 6.
http://www.digitmag.co.uk/news/index.cfm?fuseaction=displaynews&NewsID=4231
Robert McMillan

- **Cost dictates security plans**

Companies must ignore return on investment, and align security needs with the business. Businesses across the globe believe that their operations are under greater threat than ever before. But findings from the Global Information Security Survey, which questioned 7,000 business technology and security professionals in 40 countries, highlights the primitive measures being used to defend against a significant menace.
http://www.vnunet.com/features/1156593
VNUNetwork

- **Corporate weak points persist**

Vendors' legal liability regarding security flaws must be clarified
The Global Information Security Survey has highlighted the vulnerabilities felt by businesses across the globe.
Malicious attacks are more of a threat than ever before, and organisations are desperately looking to external bodies to shoulder some of the blame or find a solution to ease the burden on business.
http://www.vnunet.com/features/1156591
VNUNetwork

- **Windows vs. Linux security: No unbiased reports**

Forrester Research published a report last March that came to the unlikely conclusion that Linux is no more secure than Windows. Last month, Danish security firm Secunia compared security across operating systems and concluded that Windows was more secure than many people think. Both studies are easy to counter with a little research and common sense, but that still leaves us without any meaningful third-party operating system security assessment.
http://www.newsforge.com/article.pl?sid=04/07/06/1812203
Nicholas Petreley

New Vulnerabilities Tested in SecureScout

- **12107 Microsoft SSL library DoS and Remote Code Execution (MS04-011/835732) (SSL Safe Check on HTTP)**

A denial of service vulnerability exists in the Microsoft Secure Sockets Layer (SSL) library. The vulnerability results from the way that the Microsoft SSL library handles malformed SSL messages. This vulnerability could cause the affected system to stop accepting SSL connections on Windows 2000 and Windows XP. On Windows Server 2003, the vulnerability could cause the affected system to automatically restart.

If found vulnerable to this issue and unless you applied specific workarounds, you are also vulnerable to all other vulnerabilities described in the Microsoft Security Bulletin MS04-011.

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

CVE Links: CAN-2003-0533 & CAN-2003-0663 $ CAN-2003-0719 & CAN-2003-0806 &

CAN-2003-0906 & CAN-2003-0907 & CAN-2003-0908 & CAN-2003-0909 & CAN-2003-0910 & CAN-2004-0117 & CAN-2004-0118 & CAN-2004-0119 & CAN-2004-0120 & CAN-2004-0123

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

- **12108 Microsoft SSL library DoS and Remote Code Execution (MS04-011/835732) (SSL Safe Check on LDAP)**

A denial of service vulnerability exists in the Microsoft Secure Sockets Layer (SSL) library. The vulnerability results from the way that the Microsoft SSL library handles malformed SSL messages. This vulnerability could cause the affected system to stop accepting SSL connections on Windows 2000 and Windows XP. On Windows Server 2003, the vulnerability could cause the affected system to automatically restart.

If found vulnerable to this issue and unless you applied specific workarounds, you are also vulnerable to all other vulnerabilities described in the Microsoft Security Bulletin MS04-011.

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

CVE Links: CAN-2003-0533 & CAN-2003-0663 $ CAN-2003-0719 & CAN-2003-0806 & CAN-2003-0906 & CAN-2003-0907 & CAN-2003-0908 & CAN-2003-0909 & CAN-2003-0910 & CAN-2004-0117 & CAN-2004-0118 & CAN-2004-0119 & CAN-2004-0120 & CAN-2004-0123

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

- **14202 LSASS Buffer Overrun (MS04-011/835732) (SMB Safe Check)**

A buffer overrun vulnerability exists in LSASS that could allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take complete control of the affected system.

If found vulnerable to this issue and unless you applied specific workarounds, you are also vulnerable to all other vulnerabilities described in the Microsoft Security Bulletin MS04-011.

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

CVE Link: CAN-2003-0533 & CAN-2003-0663 $ CAN-2003-0719 & CAN-2003-0806 & CAN-2003-0906 & CAN-2003-0907 & CAN-2003-0908 & CAN-2003-0909 & CAN-2003-0910 & CAN-2004-0117 & CAN-2004-0118 & CAN-2004-0119 & CAN-2004-0120 & CAN-2004-0123

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

- **15342 ASN.1 Vulnerability Could Allow Code Execution (MS04-007/828028) (SMTP Check)**

Security vulnerability exists in the Microsoft ASN.1 Library that could allow code execution on an affected system. The vulnerability is caused by an unchecked buffer in the Microsoft ASN.1 Library, which could result in a buffer overflow.

An attacker who successfully exploited this buffer overflow vulnerability could execute code

with system privileges on an affected system. The attacker could then take any action on the system, including installing programs, viewing data, changing data, deleting data, or creating new accounts with full privileges.

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

CVE Link: CAN-2003-0818

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-007.mspx

- **17174 Apache Tomcat 3.2.1 Error Message Information Disclosure Vulnerability**

Jakarta Tomcat can be configured to display an alternate error file that is not done by default. When an exception is thrown in a Java Server Page from Jakarta Tomcat, the server displays an error page containing debugging information which includes the message of the exception that was thrown and a stack trace.
This potentially sensitive information, along with the absolute path of the JSP file on the webserver may aid in further attacks.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.securityfocus.com/archive/1/172168 & http://www.securityfocus.com/bid/3199 & http://jakarta.apache.org/tomcat/index.html

- **17578 Apache Tomcat Cross Site Scripting Vulnerability**

Apache Tomcat does not filter script embedding from links that are displayed on a server's website. A malicious webmaster can exploit this vulnerability to cause JavaScript commands or embedded scripts to be executed by any user who clicks on the hyper-link. Upon clicking on the hyper-link, Tomcat will generate an error message including the specified or embedded script. The specified or embedded scripting will be executed in the client's browser and treated as content originating from the target server returning the error message (even though the scripting may have originated at another site entirely).

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

CVE Link: CAN-2001-0829

Reference: http://jakarta.apache.org/tomcat/index.html & http://www.securityfocus.com/bid/2982 & http://www.securityfocus.com/bid/5542 & http://www.sans.org/top20/#U3

- **17606 Apache Tomcat DOS Device Name XSS Vulnerability**

Apache Tomcat is a freely available, open source web server maintained by the Apache Foundation.

When Apache Tomcat v4.0.3 is installed on Microsoft windows (only) with a default configuration, several example files are also installed. When some of these example files are requested without any input, they will return an error without sanitized the input URL.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.securityfocus.com/bid/5194 & http://www.securityfocus.com/archive/1/281360 & http://jakarta.apache.org/tomcat/

- **17803 W32/Sasser.worm Worm All versions (FTP Check)**

This worm:
* Scans random IP addresses for exploitable systems.
* Exploits the vulnerable system, by overflowing a buffer in LSASS.EXE.
* Creates a remote shell on TCP port 9996.
* Creates an FTP script named cmd.ftp on the remote host and executes it. This FTP script instructs the target victim to download and execute the worm (with the filename #_up.exe as aforementioned) from the infected host. The infected host accepts this FTP traffic on TCP port 5554 or 1023 (for W32/Sasser.worm.e).
* Spawns multiple threads, some of which scan the local class A subnet, others the class B subnet, and others completely random subnets. The destination port is TCP 445

This self-executing worm spreads by exploiting a Microsoft Windows vulnerability [MS04-011 vulnerability (CAN-2003-0533)]

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

CVE Link: CAN-2003-0533

Reference: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=125095 & http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx

- **17905 W32.Korgo.C Worm (Backdoor Connection Check)**

W32.Korgo.C is a worm that propagates by exploiting the LSASS vulnerability on TCP port 445 (as described in Microsoft Security Bulletin MS04-011) and opens a backdoor on TCP ports 113 and 3067.

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

CVE Link: CAN-2003-0533

Reference: http://securityresponse.symantec.com/avcenter/venc/data/w32.korgo.c.html & http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx

- **18002 W32.Dabber.B Worm (Backdoor Connection Check)**

W32.Dabber.B is a variant of W32.Dabber.A. This worm propagates by exploiting a vulnerability in the FTP server component of W32.Sasser.Worm and its variants.

W32.Dabber.B is based on available exploit code. It installs a backdoor on infected hosts and tries to listen on port 9898. If the attempt fails, W32.Dabber.B tries to listen on ports 9899 through 9999 in sequence until it finds an open port.

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

CVE Link: CAN-2003-0533

Reference: http://securityresponse.symantec.com/avcenter/venc/data/w32.dabber.b.html & http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx

New Vulnerabilities found this Week

- **Mozilla Fails to Restrict Access to "shell:"**

"use Windows "shell:" functionality"

Joshua Perrymon has reported a vulnerability in Mozilla, Mozilla Firefox, and Mozilla Thunderbird, allowing malicious websites to use Windows "shell:" functionality.

The problem is that Mozilla fails to restrict access to the "shell:" URI handler. This allows websites to invoke various programs associated with specific extensions. It is not possible to pass parameters to these programs, only filenames, thus limiting the impact of launching applications.

However, if this issue is combined with an error or a vulnerability in an associated program, it may be possible to execute arbitrary code. Reportedly, this may be possible via a buffer overflow in "WINDOWS\System32\grpconv.exe", which by default is associated with the ".grp" extension. However, only unicode characters can be used, causing exploitation to be more difficult.

The error in the associated program does not necessarily need to be classified as a vulnerability, as certain programs aren't designed or meant to be launched in a hostile environment - such as through a website and a browser.

The vulnerability affects Mozilla, Mozilla Firefox, and Mozilla Thunderbird on the Microsoft Windows XP platform due to the way the "shell:" URI handler is used and implemented on Windows XP.

The shell: URI handler is inherently insecure and should only be accessed from a few trusted sites - or not from a browser at all. Multiple exploits in Internet Explorer also utilise "shell:" functionality.

References : http ://www.mozilla.org/security/shell.html

- **MySQL Authentication Vulnerabilities**

"gain access to the database or the local system"

Chris Anley has reported two vulnerabilities in MySQL, allowing malicious people to gain access to the database or the local system.

1) MySQL fails to properly verify passwords if the client has set a specific client capability flag and specifies a "passwd_len" of NULL. This causes MySQL to accept a NULL password

as a valid password and authenticates the user.

Successful exploitation requires that the attacker knows a valid username.

2) A boundary error within the handling of "scramble" strings can reportedly be exploited to execute arbitrary code if the attacker knows a password hash or through brute forcing.

The vulnerabilities only affect beta / developement branches of MySQL 4.1.x and MySQL 5.

NOTE: Secunia doesn't recommend installing beta and development software on production systems and doesn't normally issue advisories regarding such software. However, an exception has been made in this case due to the potential attention this issue may receive.

References : http://www.nextgenss.com/advisories/mysql-authbypass.txt

- **Linux Kernel HbaApiNode Improper File Permissions Denial of Service Vulnerability**

"local attacker to cause a denial of service"

A vulnerability has been identified in the SuSE Linux kernel that may allow a local attacker to cause a denial of service condition on a vulnerable system. The issue is reported to be caused by improper file permissions on '/proc/scsi/qla2300/HbaApiNode' file.

SuSE Linux Enterprise Server 8.0, SuSE Linux 8.1 and 9.0 are reported to be affected by this issue as well as other linux operating systems.

According to a RedHat advisory, this issue also affects Fedora Core 1.

Due to a lack of details, further information cannot be provided at the moment. This BID will be updated as more information becomes available.

References : http://www.securityfocus.com/bid/10279

- **PureFTPd Accept_Client Remote Denial of Service Vulnerability**

"denial of service vulnerability"

PureFTPd is reported prone to a remote undisclosed denial of service vulnerability. The vulnerability is reported to exist due to a bug in the accept_client function used to setup new connections. It is reported that when the maximum number of connections is reached an attacker may be able to deny service to the affected daemon.

It is reported that all versions of cPanel are also affected by this issue because cPanel ships with PureFTPd 1.0.12.

References : http://www.securityfocus.com/bid/10664/discussion/

- **Horde IMP Email Header HTML Injection Vulnerability**

"email header HTML injection vulnerability"

Horde IMP is reported to be prone to an email header HTML injection vulnerability. This issue is due to a failure of the application to properly sanitize user-supplied email header strings.

An attacker can exploit this issue to gain access to an unsuspecting user's cookie based authentication credentials; disclosure of personal email is possible. Other attacks are also possible.

References : http://www.securityfocus.com/bid/10501/discussion/

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