netVigilance

ScoutNews Team **March 18, 2005**
Issue # 11

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Hacking is tuning into big business, either keep employees happy or keep your network protected and test frequently for rootkit vulnerabilities.

Enjoy reading

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

- **Hackers focusing more on profit rather than simply wreaking havoc.**

The last quarter of 2004 saw a sharp increase in the number of Spyware attacks targeted at collecting passwords, pins, account numbers and other sensitive information that could be used to perpetrate fraud.

Gartner reported at the RSA Conference in San Francisco, that 9.5 million people fell victim to online fraud. The estimated losses were calculated to be $1.2 billion.

More sophisticated methods of account authentication are called for in order to turn this trend around.

PC Magazine

Related Links:

http://www.pcmag.co.uk/news/1161793

http://www.pcmag.co.uk/news/1161282

- **Disgruntled former employees easily exploit security holes.**

A former employee of Kaiser-Permanente exposes customer records to the internet to demonstrate lax security of her former employer and in an older case, a former employee of Manufacturing Electronic Sales (MESC) gets a 5-month sentence / $45k fine.

Unauthorized intrusion by disgruntled employees or former employees, still remains the leading source of hacker attack.

Related Links:
http://www.nwfusion.com/news/2005/0316kaiseperma.html
http://www.nwfusion.com/news/2005/0315itmanag.html
http://www.theregister.co.uk/2005/03/17/industrial_cyber-security/

- **Rootkits pose serious new threat, easy to obtain.**

Rootkits; programs that replace operating systems functions with malicious copies that allow hackers back door entry. Since they dwell deep within the operating system, they can hide the very characteristics that would disclose them to anti-virus software.

The recent Myfip.H and Maslan viruses have used characteristics of rootkits to mask their presence.

SecureScout has rootkit detection testcase included. Contact support to get a list of rootkit specific tests.

Related Link:
http://www.nwfusion.com/news/2005/0315compalinin.html

New Vulnerabilities Tested in SecureScout

❖ 13197 MySQL "udf_init()" function Vulnerability

An input validation error in the "udf_init()" function in "sql_udf.cc" causes the "dl" field of the "mysql.func" table to not be properly sanitised before being used to load libraries. This can be exploited by manipulating the "mysql" administrative database directly via a "INSERT INTO" statement instead of using "CREATE FUNCTION".

Successful exploitation allows loading a malicious library from an arbitrary location, but requires "INSERT" and "DELETE" permissions on the "mysql" administrative database.

The vulnerabilities have been reported in versions 4.0.23, and 4.1.10 and prior.

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

References:

Original advisories:
http://archives.neohapsis.com/archives/vulnwatch/2005-q1/0084.html
http://archives.neohapsis.com/archives/vulnwatch/2005-q1/0083.html
http://archives.neohapsis.com/archives/vulnwatch/2005-q1/0082.html

Other references:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0709
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0710
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0711

Vendor:
http://www.mysql.com/

CVE Reference: CAN-2005-0709 CAN-2005-0710 CAN-2005-0711

❖ 13198 MySQL "CREATE TEMPORARY TABLE" command Vulnerability

Temporary files are created insecurely with the "CREATE TEMPORARY TABLE" command and can be exploited via symlink attacks to overwrite arbitrary files with the privileges of MySQL.

The vulnerabilities have been reported in versions 4.0.23, and 4.1.10 and prior.

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

References:

Original advisories:

http://archives.neohapsis.com/archives/vulnwatch/2005-q1/0084.html
http://archives.neohapsis.com/archives/vulnwatch/2005-q1/0083.html
http://archives.neohapsis.com/archives/vulnwatch/2005-q1/0082.html

Other references:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0709
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0710
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0711

Vendor:
http://www.mysql.com/

CVE Reference: CAN-2005-0709 CAN-2005-0710 CAN-2005-0711

❖ 13199 MySQL MS-DOS Device Names Denial of Service Vulnerability

The vulnerability is caused due to an error in the handling of reserved MS-DOS device names. This can be exploited to cause a crash by changing to a database with a specially crafted name.

Example:
use LPT1;

Successful exploitation requires global privileges (on *.*) for any of the following commands:
* REFERENCES
* CREATE TEMPORARY TABLES
* GRANT OPTION
* CREATE
* SELECT

The vulnerability has been reported in versions 4.0.x and 4.1.x for Windows.

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

References:

Original advisories:
http://bugs.mysql.com/bug.php?id=9148

Vendor:
http://www.mysql.com/

CVE Reference: none.

❖ 13207 MySQL mysqlaccess Script Insecure Temporary File Creation Vulnerability

Javier Fernández-Sanguino Peña has reported a vulnerability in MySQL, which can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges.

The vulnerability is caused due to the mysqlaccess script creating temporary files insecurely. This can be exploited via symlink attacks to overwrite or disclose the content of arbitrary files with the privileges of the user running the vulnerable script.

Affects versions 3.23.49/4.0.23/4.1.9/5.0.2 and earlier.

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

References:

Original advisories:
http://www.debian.org/security/2005/dsa-647
http://marc.theaimsgroup.com/?l=bugtraq&m=110608297217224&w=2

Other references:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0004
http://xforce.iss.net/xforce/xfdb/18922

Vendor:
http://www.mysql.com/

CVE Reference: CAN-2005-0004

❖ 13208 MySQL "ALTER TABLE ... RENAME" Vulnerability

An error in "ALTER TABLE ... RENAME" operations causes the CREATE/INSERT rights of old tables to be checked, which potentially can be exploited to bypass some applied security restrictions.

The vulnerability has been reported in version 3.23. Other versions may also be affected.

Affects versions 3.23.58 and earlier.

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

References:

Original advisories:
http://bugs.mysql.com/bug.php?id=3270
http://bugs.mysql.com/bug.php?id=2408

http://bugs.mysql.com/bug.php?id=3870
http://bugs.mysql.com/bug.php?id=3933

Other references:
http://dev.mysql.com/downloads/mysql/

Vendor:
http://www.mysql.com/

CVE Reference: CAN-2004-0835 CAN-2004-0837 CAN-2004-0957

❖ 13209 MySQL stalling server Vulnerability

It is possible to crash or stall the server when multiple threads ALTER the same or different MERGE tables to change the UNION.

The vulnerability has been reported in version 3.23 and 4.0.18. Other versions may also be affected.

Affects versions 3.23.58 and earlier.
Affects versions 4.0.18 and earlier.

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

References:

Original advisories:
http://bugs.mysql.com/bug.php?id=3270
http://bugs.mysql.com/bug.php?id=2408
http://bugs.mysql.com/bug.php?id=3870
http://bugs.mysql.com/bug.php?id=3933

Other references:
http://dev.mysql.com/downloads/mysql/

Vendor:
http://www.mysql.com/

CVE Reference: CAN-2004-0835 CAN-2004-0837 CAN-2004-0957

❖ 13210 MySQL double quote in an AGAINST function Vulnerability

It is possible to crash the MySQL server via a specially crafted SELECT statement containing a double quote in an AGAINST function.

The vulnerability has been reported in version 4.0.20. Other versions may also be affected.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Medium** Risk: **DoS**

References:

Original advisories:
http://bugs.mysql.com/bug.php?id=3270
http://bugs.mysql.com/bug.php?id=2408
http://bugs.mysql.com/bug.php?id=3870
http://bugs.mysql.com/bug.php?id=3933

Other references:
http://dev.mysql.com/downloads/mysql/

Vendor:
http://www.mysql.com/

CVE Reference: CAN-2004-0835 CAN-2004-0837 CAN-2004-0957

- **13211 MySQL grant privileges on a database Vulnerability**

An error when checking privileges can be exploited under certain conditions to grant privileges on a database, which the user has no privileges on.

The vulnerability has been reported in version 4.0.20. Other versions may also be affected.

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

References:

Original advisories:
http://bugs.mysql.com/bug.php?id=3270
http://bugs.mysql.com/bug.php?id=2408
http://bugs.mysql.com/bug.php?id=3870
http://bugs.mysql.com/bug.php?id=3933

Other references:
http://dev.mysql.com/downloads/mysql/

Vendor:
http://www.mysql.com/

CVE Reference: CAN-2004-0835 CAN-2004-0837 CAN-2004-0957

- **15176 Firefox "Save Link As..." Status Bar Spoofing Weakness (Remote File Checking)**

bitlance winter has discovered a weakness in Firefox, which can be exploited by malicious people to trick users into saving malicious files by obfuscating URLs.

The status bar cannot be manipulated via script code in the default settings. However, it is still possible to display an incorrect URL in the status bar when hovering the mouse over a link, right clicking, and choosing "Save Link As...".

This can be exploited by including a nested link in a table inside a link.

The weakness has been confirmed in version 1.0.1. Other versions may also be affected.

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

References:

Original Advisory:
http://secunia.com/advisories/14565/

Product HomePage:
http://www.mozilla.org/products/firefox/

Other references:
http://secunia.com/advisories/1301

CVE Reference: none.

❖ 15177 Thunderbird "Save Link Target As..." Status Bar Spoofing Weakness (Remote File Checking)

bitlance winter has discovered a weakness in Thunderbird, which can be exploited by malicious people to trick users into saving malicious files by obfuscating URLs.

The status bar cannot be manipulated via script code in the default settings. However, it is still possible to display an incorrect URL in the status bar when hovering the mouse over a link, right clicking, and choosing "Save Link As...".

This can be exploited by including a nested link in a table inside a link.

The weakness has been confirmed in version 1.0. Other versions may also be affected.

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

References:

Original Advisory:

http://secunia.com/advisories/14567/

Product HomePage:
http://www.mozilla.org/products/firefox/

Other references:
http://secunia.com/advisories/13015/

CVE Reference: none.

- **15178 Mozilla "Save Link Target As..." Status Bar Spoofing Weakness (Remote File Checking)**

bitlance winter has discovered a weakness in Mozilla, which can be exploited by malicious people to trick users into saving malicious files by obfuscating URLs.

The status bar cannot be manipulated via script code in the default settings. However, it is still possible to display an incorrect URL in the status bar when hovering the mouse over a link, right clicking, and choosing "Save Link Target As...".

This can be exploited by including a nested link in a table inside a link.

The weakness has been confirmed in version 1.7.5. Other versions may also be affected.

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

References:

Original Advisory:
http://secunia.com/advisories/14568/

Product HomePage:
http://www.mozilla.org/products/firefox/

Other references:
http://secunia.com/advisories/13015/

CVE Reference: none.

New Vulnerabilities found this Week

- **Novell iChain miniFTP Server Brute Force Weakness**

“brute force a user's password”

Francisco Amato has reported a weakness in Novell iChain, which can be exploited by malicious people to potentially brute force a user's password.

The problem is that the miniFTP server does not limit the number of invalid logins nor logs these. This may eventually allow a malicious person to guess a valid password.

The miniFTP server reportedly also returns error messages when an invalid username is supplied.

The weakness has been reported in version 2.3. Other versions may also be affected.

References:

http://support.novell.com/cgi-bin/search/searchtid.cgi?/10096887.htm

❖ **Symantec Products Unspecified DNS Cache Poisoning Vulnerability**

“poison the DNS cache”

A vulnerability has been reported in various Symantec gateway products, which can be exploited by malicious people to poison the DNS cache.

The vulnerability is caused due to an unspecified error in the DNS proxy (DNSd) when functioning as a DNS caching server or primary DNS server and can be exploited to poison the DNS cache.

The following products are affected:
* Symantec Gateway Security 5400 Series, v2.x
* Symantec Gateway Security 5300 Series, v1.0
* Symantec Enterprise Firewall, v7.0.x (Windows and Solaris)
* Symantec Enterprise Firewall v8.0 (Windows and Solaris)
* Symantec VelociRaptor, Model 1100/1200/1300 v1.5

NOTE: This has already been exploited in the wild.

References:

http://securityresponse.symantec.com/avcenter/security/Content/2005.03.15.html

http://service1.symantec.com/support/ent-gate.nsf/docid/2005030417285454

❖ **Linux Kernel PPP Server Denial of Service Vulnerability**

"Denial of Service"

Ben Martel and Stephen Blackheath have reported a vulnerability in the Linux kernel, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the LCP (Link Control Protocol) parsing in the "ppp_async.c" driver and can be exploited by pppd clients to cause the server to hang.

References:

http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.4

❖ **KDE Desktop Communication Protocol Denial of Service Vulnerability**

"Denial of Service"

Sebastian Krahmer has reported a vulnerability in KDE, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the authentication process in the DCOP (Desktop Communication Protocol) daemon dcopserver. This can be exploited to lock the dcopserver for arbitrary local users.

Successful exploitation may result in decreased desktop functionality for the affected user.

The vulnerability has been reported in versions prior to 3.4.

References:

http://www.kde.org/info/security/advisory-20050316-1.txt

❖ **Citrix MetaFrame Password Manager Secondary Password Disclosure**

"gain knowledge of potentially sensitive information"

A security issue has been reported in MetaFrame Password Manager, which can be exploited by malicious users to gain knowledge of potentially sensitive information.

An administrator can define a policy to prevent users from viewing their own secondary application passwords. However, it is still possible to gain knowledge of the passwords, since they can be extracted in plain text from pages displaying them as a series of asterisks.

References:

http://support.citrix.com/kb/entry.jspa?entryID=5970&categoryID=254

❖ **WebSphere Commerce Private Information Disclosure**

"sensitive information being disclosed to malicious people"

A security issue has been reported in WebSphere Commerce, which may result in sensitive information being disclosed to malicious people.

Under certain circumstances when using servlet caching, the cache entry for a product or category display page can become linked to a prepolutated form, which may disclose private information.

The security issue has been reported in versions 5.5, 5.6, and 5.6.0.1.

References:

http://www-1.ibm.com/support/docview.wss?uid=swg21199839

❖ **Apache Tomcat AJP12 Protocol Denial of Service Vulnerability**

"Denial of Service"

Hitachi Incident Response Team has reported a vulnerability in Tomcat, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the servlet / JSP communication handling for the AJP12 protocol. This can be exploited to cause a vulnerable server to stop processing further requests by sending a specially crafted request to the APJ12 protocol port (8007/tcp by default).

The vulnerability has been reported in version 3.x.

References:

http://www.kb.cert.org/vuls/id/204710

❖ **Linux Kernel "sys_epoll_wait()" Function Integer Overflow**

"gain escalated privileges"

Georgi Guninski has reported a potential vulnerability in the Linux kernel, which may be exploited by malicious people to gain escalated privileges.

The vulnerability is caused due to an integer overflow in the "sys_epoll_wait()" function and can be exploited to cause a buffer overflow overwriting low kernel memory.

Successful exploitation may potentially allow execution of arbitrary code with escalated privileges. However, few applications reportedly use the affected part of the kernel memory space.

The vulnerability has been reported in versions 2.6 through 2.6.11.

References:

http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.2

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