netVigilance

ScoutNews Team **May 20 2005**
Issue # 20

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Although it is not a new brand of toothpaste; Microsoft is hoping OneCare will be preferred by 4 out of 5 PC users in preventing cavities and buildup. From the 'You can't make this stuff up' files – hackers now shaking down e-commerce vendors to prevent them from launching an attack. Data encryption for the masses and Homeland WAN (in)Security.

Enjoy reading & Stay Secure

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

Top Security News Stories this Week

- **Identity Based Encryption (IBE) from Voltage Security, makes public-key encryption easy to manage.**

Voltage has developed technology that enables users to define public keys based on easy-to-remember numbers, words or strings such as email addresses. This will allow non-expert users to establish encryption for common data transmissions such as email and file sharing.

redherring

Related Links :

http://www.redherring.com/Article.aspx?a=12088&hed=RH-100:+Democratizing+Encryption

http://www.voltage.com/index.htm

❖ FEDS doing poor job on wireless security

The GAO reported on Tuesday findings that Government agencies are rapidly deploying wireless LAN capabilities with little or no attention to the security of these networks. All six of the agencies tested showed abysmal security policies for WLANs.

Out-Law.com

Full Story:
http://www.out-law.com/php/page.php?page_id=fedsbotchwireless1116507313&area=news

❖ Microsoft OneCare enters beta testing; carving into security S/W market

Coinciding with the release of the latest Star Wars saga; the Redmond empire boldly outlines a strong push to take over portions of the security universe. OneCare touts automated updates of antivirus, disaster recovery and PC tune-ups and has sent shudders to established desktop security companies.

Any similarities drawn between big M and any of the opposing forces in the latest Lucas tale; will be left entirely up to the reader. Nonetheless, this appears to be the beginnings of an epic battle for the hearts and minds of the rest of us inhabitants of the internet cosmos.

RedHerring

Related Links:
http://www.redherring.com/Article.aspx?a=12071&hed=Microsoft+Tests+Security+System&sector=Industries&subsector=SecurityAndDefense

http://www.microsoft.com/windows/onecare/default.mspx

❖ Net shakedowns becoming a real threat

In a bizarre story that reads like a script from a gangster movie; e-commerce companies are falling victim to extortion scams where hackers send a notice threatening to shut down the company's website unless they are paid.

The hackers typically demonstrate their capabilities by launching an initial DoS attack.

Network World

Full Story:

http://www.networkworld.com/weblogs/security/008861.html

New Vulnerabilities Tested in SecureScout

❖ 13235 MySQL mysql_install_db Insecure Temporary File Creation Vulnerability

Eric Romang has reported a vulnerability in MySQL, which can be exploited by malicious, local users to conduct various actions on a vulnerable system with escalated privileges.

The vulnerability is caused due to the mysql_install_db script creating the temporary file "mysql_install_db.$$" insecurely. This can be exploited to overwrite arbitrary files with the privileges of the user running the vulnerable script via symlink attacks or execute arbitrary SQL commands by manipulating the file's contents.

The vulnerability has been reported in versions 4.1.11 and prior and development release 5.0.4 and prior.

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

References:

Original advisories:
http://www.zataz.net/adviso/mysql-05172005.txt

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

Other references:
http://secunia.com/advisories/15369/

CVE Reference: CAN-2005-1636

❖ 15194 Fastream NETFile FTP/Web Server FTP Bounce Vulnerability (Remote File Checking)

Tan Chew Keong has reported a vulnerability in Fastream NETFile FTP/Web Server, which potentially can be exploited by malicious users to bypass certain security restrictions.

The vulnerability is caused due to missing validation of the IP address specified as argument to the PORT command and can be exploited via so-called "FTP Bounce" attacks to open connections to arbitrary systems via the FTP server.

Successful exploitation may allow bypassing of firewall filters and access systems, which would otherwise be inaccessible.

This can also be exploited further to cause a DoS (Denial of Service) by uploading a specially crafted text file or access the admin interface (port 30000/tcp).

The vulnerability has been reported in version 7.4.6. Other versions may also be affected.

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

References:

Original Advisory:
http://www.security.org.sg/vuln/netfileftp746port.html

Other references:
http://www.cert.org/advisories/CA-1997-27.html
http://secunia.com/advisories/15394/

CVE Reference: CAN-2005-1646

❖ 15195 Fastream NETFile FTP/Web Server Multiple HEAD Requests Denial of Service (Remote File Checking

bratax has reported a vulnerability in Fastream NETFile FTP/Web Server, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the "Keep-Alive" connection timeout handling. The problem is that the web server doesn't close connections to clients when receiving HTTP HEAD requests.

This can be exploited to consume all available connections and prevent further connections from being established by sending multiple HTTP HEAD requests.

The vulnerability has been reported in version 7.12. Prior versions may also be affected.

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

References:

Original Advisory:
http://users.pandora.be/bratax/advisories/b003.html

Other references:
http://secunia.com/advisories/13268/

CVE Reference: None

❖ 15196 Fastream NETFile FTP/Web Server Directory Traversal Vulnerability (Remote File Checking)

aT4r ins4n3 has reported a vulnerability in Fastream NETFile FTP/Web Server, which can be exploited by malicious people to retrieve or overwrite arbitrary files.

Input passed to the "filename" parameter isn't properly verified before it is used in various commands. This can be exploited by using two slashes ("..//") in a classical directory traversal attack through various commands to view and overwrite files.

The vulnerability has been reported in version 6.7.2.1085. Prior versions may also be affected.

NOTE: Tan Chew Keong has reported that it is possible to bypass the sanitisation and verification process in version 7.4.6, using e.g. the ".../..//a/.../" character sequence in a directory traversal attack. Other versions may also be affected.

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

References:

Original Advisory:
http://www.haxorcitos.com/Fastream_advisory.txt
http://www.security.org.sg/vuln/netfileftp746.html

Other references:
http://secunia.com/advisories/12016/

CVE Reference: CAN-2004-0676

❖ 15197 Fastream NETFile FTP/Web Server Invalid Credentials Denial of Service (Remote File Checking)

Donato Ferrante has reported a vulnerability in Fastream NETFile FTP/Web Server, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is reportedly caused due to an error within the login procedure of the FTP server. This may result in the FTP server crashing when receiving invalid user credentials.

The vulnerability has been reported in version 6.5.1.980. Prior versions may also be affected.

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

References:

Original Advisory:
http://www.autistici.org/fdonato/advisory/FastreamNETFileFWServer6.5.1.980-adv.txt

Other references:
http://secunia.com/advisories/11428/

CVE Reference: None

❖ 15198 Fastream NetFile FTP/WebServer Cross-Site Scripting Vulnerability (Remote File Checking)

A vulnerability has been reported in Fastream NetFile FTP/WebServer, which can be exploited by malicious people to conduct Cross-Site Scripting attacks against other visitors.

The problem is that error pages include requested URLs without prior sanitation. This can be exploited by including arbitrary HTML or script code, which can be executed in another user's browser session when viewed.

Example:
http://[victim]/<script>alert(document.cookie)</script>

The vulnerability has been reported in version 6.0.

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

References:

Original Advisory:
http://secunia.com/advisories/10099/

CVE Reference: None

❖ 15199 ignitionServer Access Entry Deletion Vulnerability (Remote File Checking)

A vulnerability has been reported in ignitionServer, which can be exploited by malicious users to delete access entries.

According to the IRCX draft, only owners are allowed to delete access entries set by owners. However, this is not checked before access entries are deleted, which breaches channel security and allows hosts to delete access entries set by owners.

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

References:

Original Advisory:
http://www.ignition-project.com/security/20050414-hosts-delete-owner-access-entries
http://www.ignition-project.com/security/20050515-protected-opers-cannot-join-channel-with-key

Other references:
http://secunia.com/advisories/15388/

CVE Reference: CAN-2005-1640, CAN-2005-1641

❖ 15200 ignitionServer Channel Locking Vulnerability (Remote File Checking)

A vulnerability has been reported in ignitionServer, which can be exploited by malicious users to prevent protected operators from accessing certain channels.

Due to a design error, protected IRC operators can't access channels created and locked by normal users.

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

References:

Original Advisory:
http://www.ignition-project.com/security/20050414-hosts-delete-owner-access-entries
http://www.ignition-project.com/security/20050515-protected-opers-cannot-join-channel-with-key

Other references:
http://secunia.com/advisories/15388/

CVE Reference: CAN-2005-1640, CAN-2005-1641

❖ 15201 ignitionServer "SERVER" Denial of Service Vulnerability (Remote File Checking)

A vulnerability has been reported in ignitionServer, which can be exploited by malicious people to cause a DoS (Denial of Service) on vulnerable systems.

The vulnerability is caused due to insufficient restrictions on the "SERVER" command. The command is designed for server to server communication, but can be exploited by clients to introduce non-existing servers to the network.

This can further be exploited to cause a DoS by introducing multiple servers, which can potentially flood the network.

The vulnerability reportedly affect versions 0.1.2 through 0.3.1.

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

References:

Original Advisory:
http://secunia.com/advisories/12374/

CVE Reference: None

❖ 15202 ignitionServer Server Linking Password Verification Vulnerability (Remote File Checking)

A vulnerability has been discovered in ignitionServer, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to missing password verification when linking servers.

Successful exploitation requires use of linking, which is currently experimental, and allows the password restriction to be bypassed. The full impact is reportedly unknown.

The vulnerability has been reported in versions 0.1.2 through 0.3.1.

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

References:

Original Advisory:
http://secunia.com/advisories/11824/

CVE Reference: None

New Vulnerabilities found this Week

- ❖ **Cisco Various Products TCP Timestamp Denial of Service**
  "Denial of Service"

  A vulnerability has been reported in some Cisco products, which can be exploited by malicious people to cause a DoS (Denial of Service) on active TCP sessions.

  The vulnerability is caused due to an error in the implementation of the TCP Timestamp option and can be exploited via specially crafted packets to cause a targeted TCP session to stall until it's reset.

  Successful exploitation requires knowledge of IP address information of the source and destination of the TCP network connection.

  The vulnerability affects the following products:
  * SN5400 series storage routers
  * CSS11000 series content services switches
  * AP350 and AP1200 series Access Points running VxWorks
  * MGX8200, MGX8800, and MGX8900 series WAN switches (only management interfaces)

  References:
  http://www.cisco.com/warp/public/707/cisco-sn-20050518-tcpts.shtml
  http://www.kb.cert.org/vuls/id/637934

- ❖ **MySQL mysql_install_db Insecure Temporary File Creation**
  "Overwrite arbitrary files"

  Eric Romang has reported a vulnerability in MySQL, which can be exploited by malicious, local users to conduct various actions on a vulnerable system with escalated privileges.

  The vulnerability is caused due to the mysql_install_db script creating the temporary file "mysql_install_db.$$" insecurely. This can be exploited to overwrite arbitrary files with the privileges of the user running the vulnerable script via symlink attacks or execute arbitrary SQL commands by manipulating the file's contents.

The vulnerability has been reported in versions 4.1.11 and prior and development release 5.0.4 and prior.

References:
http://www.zataz.net/adviso/mysql-05172005.txt

- ❖ **FreeRADIUS Potential SQL Injection and Buffer Overflow Vulnerabilities**

"SQL injection attacks"

Primoz Bratanic has reported some vulnerabilities in FreeRADIUS, where one has an unknown impact and the others potentially can be exploited by malicious users to conduct SQL injection attacks.

1) A boundary error in the "sql_escape_func()" function in rlm_sql.c can potentially be exploited to cause a buffer overflow via specially crafted input that needs escaping.

It has been speculated that successful exploitation may allow execution of arbitrary code, but this has not been proven.

2) Missing sanitation when calling the "radius_xlat()" function in rlm_sql.c can potentially be exploited by authenticated users to manipulate SQL queries by injecting arbitrary SQL code.

References:
http://security.gentoo.org/glsa/glsa-200505-13.xml

- ❖ **Linux Kernel pktcdvd and raw device Block Device Vulnerabilities**

"Gain escalated privileges"

alert7 has reported two vulnerabilities in the Linux kernel, which can be exploited by malicious, local users to gain escalated privileges.

Input validation errors in the raw device and pktcdvd block device ioctl handlers (raw_ioctl() and pkt_ioctl() functions) can be exploited to corrupt kernel memory via specially crafted arguments passed to the ioctl_by_bdev() function.

Successful exploitation allows execution of arbitrary code with kernel level privileges, but requires that the user can read the affected block device.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.10

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