**ScoutNews Team** **August 5, 2005**
**Issue # 31**

Weekly ScoutNews by netVigilance

**Table of Contents**



## This Week in Review

It's been a busy week – Use SecureScout to find out if you are protected against the Mike Lynn Cisco router flaw, Microsoft touts success of 'Blue Hat' conference, Vista already gets hacked, Virus' infect Bluetooth-capable cars and Mozilla talks of profit?

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

- **SecureScout contains tests for Lynn Cisco flaws**

The SecureScout test case database has contained test for the vulnerabilities outlined by Mike Lynn at the Black Hats conference since as early as January '05. The vulnerability described in the Lynn presentation is based on IPv6, so I will say that using TestCase 15576 is the best reference. As long as you perform regular assessments and remediation, the sky is not going to fall – Ed.

Relevant SecureScout testcases:

```
15591 Cisco IOS IKE XAUTH Implementation Security Bypass
      Vulnerabilities (CSCin82407/CSCeg00277)   April 7, 2005
15592 Cisco IOS Secure Shell Server Denial of Service Vulnerabilities
      (CSCed65778/CSCed65285)       April 7, 2005
```

```
15575 Cisco IOS BGP Protocol Processing Denial of Service Vulnerability
      (CSCee67450)                  January 27, 2005
15576 Cisco IOS IPv6 Packet Processing Denial of Service Vulnerability
      (CSCee67450)                        January 27, 2005
15577 Cisco IOS MPLS Packet Processing Denial of Service Vulnerability
      (CSCee67450)                        January 27, 2005
```

Related Links:

http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml

http://www.betanews.com/article/Cisco_Router_Flaw_Goes_Public/1122575077

### ❖ Color me Black and Blue - Microsoft spawns Blue Hat conference

In March Microsoft hosted the 'Blue Hat' conference, inviting hackers to it's Redmond campus to demonstrate their craft before developers and execs. Microsoft was so pleased with the success, so they are considering making this a bi-annual event. The Blue Hat event's name is a reference to the annual Black Hat security conference, with the color in the title changed to blue because that's the color of the badges Microsoft employees wear on campus

Yahoo

Full Story :
http://news.yahoo.com/s/pcworld/20050802/tc_pcworld/122070%3b_ylt=A9FJqY0U1.9CJUIA1QOs0NUE%3b_ylu=X3oDMTA3cjE0b2MwBHNlYwM3Mzg-

### ❖ Microsoft Vista has pre-release vulnerabilities

Like flies to a Honeypot, hackers pounced on the beta release of Vista and have already published potential exploits. The proof-of-concept virus' target the new command line interface (CLI); Monad. Monad is a CLI and scripting language that is similar to Unix shells such as BASH.

According to Mikko Hyppönen, the director of antivirus research at F-Secure, the Monad viruses were written by a virus writer who calls himself "Second Part To Hell" (I know; scary. I somehow missed the First part – Ed.)

ZDNet

Related Links:

http://www.i4u.com/article3973.html

http://news.zdnet.co.uk/0,39020330,39212024,00.htm

- **Latest Bluetooth hack leaves driver 'hearing voices'**

This one writes itself; a group know as Trifinite Group released 'Car Whisperer' virus that can easily infect Bluetooth systems on a large number of automobile; generating audio messages to drivers.

Although the entertainment value far exceeds any real threats in the wild, it does raise the concern for more serious and potentially dangerous virus' in the future.
Yahoo

Related Links:
http://news.yahoo.com/news?tmpl=story&u=/pcworld/20050803/tc_pcworld/122077

- **Mozilla going 'commerc'**

In a surprise announcement, Mozilla plans to form a for-profit subsidiary to commercialize it's popular freeware tools such as Firefox and Thunderbird. Mitchell Baker, the new Mozilla Corporation President was quoted commenting about the new corporate entity "[it] is granted greater legal freedom and can more easily interact with other corporate entities." ?
Yahoo

Related Links:
http://www.windowsitpro.com/Article/ArticleID/47219/47219.html

# New Vulnerabilities Tested in SecureScout

- **13272 Oracle Database Server - Oracle HTTP Server (mod_ssl) component Unspecified error (jul-2005/DB11)**

An unspecified error in the Oracle HTTP Server (mod_ssl) component can potentially be exploited to disclose or manipulate information.

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

**References:**

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujul2005.html

Product Homepage:
http://www.oracle.com/

**CVE Reference:** None

### ❖ 13274 MySQL zlib library Vulnerabilities

Some vulnerabilities have been reported in MySQL, which can be exploited by malicious users to cause a DoS (Denial of Service), or potentially by malicious people to execute arbitrary code.

MySQL uses a vulnerable version of the zlib library.

A vulnerability has been reported in zlib, which can be exploited by malicious people to conduct a DoS (Denial of Service) against a vulnerable application, or potentially to execute arbitrary code.

The vulnerability is caused due to a boundary error in "inftrees.c" when handling corrupted compressed data streams. This can be exploited to crash any application that uses the zlib library, or potentially to execute arbitrary code with privileges of the vulnerable application.

Versions of MySQL 4.x up to and including 4.1.12 are vulnerable.

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

**References:**

Original advisories:
http://dev.mysql.com/doc/mysql/en/news-4-1-13.html

Other references:
http://secunia.com/advisories/16170/
http://secunia.com/SA15949/

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

**CVE Reference:** CAN-2005-2096

### ❖ 15657 AOL Instant Messenger Escaped Character Entities DoS Vulnerability (Remote File Checking)

The remote host is using AOL Instant Messenger (AIM) - a p2p software, which may not be suitable for a business environment.

Escaped character entities ranging from &#770 - &#779 sent to an AOL Instant Messenger client have varying effects ranging from closing of message windows to shutdown of the application. Attacks can be launched if URL references contain these particular entities. Restart of the application is required in order to regain normal functionality.

Vulnerable: AOL Instant Messenger 3.5.1808

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

**References:**

Original advisory:
http://www.securityfocus.com/bid/1810

Product HomePage:
http://www.aim.com/get_aim/win/latest_win.adp

**CVE Reference:** None

### ❖ 15658 AOL Instant Messenger Buffer Overflow Vulnerability (Remote File Checking)

The remote host is using AOL Instant Messenger (AIM) - a p2p software, which may not be suitable for a business environment.

Certain versions of Americal Online's Instant Messenger client are vulnerable to a buffer overflow attack.

By modifying incoming packets, it is possible for an attacker with sufficient skills, and access to the network between the affected client and the AOL Instant Messenger server to cause a buffer overflow condition in the IM client, permitting a remote attacker to execute arbitrary code.

Vulnerable: AOL Instant Messenger 2.1.1236

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

**References:**

Original advisory:
http://www.securityfocus.com/bid/2236

Product HomePage:
http://www.aim.com/get_aim/win/latest_win.adp

**CVE Reference:** None

### ❖ 15662 Firefox "InstallVersion.compareTo()" function Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox, which can be exploited by malicious people to bypass certain security restrictions, conduct cross-site scripting attacks, and compromise a user's system.

An input validation error in the handling of unexpected JavaScript objects passed to the "InstallVersion.compareTo()" function may be exploited to execute arbitrary code.

This vulnerability affects versions up to and including 1.0.4.

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

**References:**

Original advisory:
http://www.mozilla.org/security/announce/mfsa2005-50.html

Other references:
http://secunia.com/advisories/14938/
http://secunia.com/advisories/16043/

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

**CVE Reference:** CAN-2005-2260, CAN-2005-2261, CAN-2005-2262, CAN-2005-2263, CAN-2005-2264, CAN-2005-2265, CAN-2005-2267, CAN-2005-2269, CAN-2005-2270

### ❖ 15663 Firefox "javascript:" URIs Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox, which can be exploited by malicious people to bypass certain security restrictions, conduct cross-site scripting attacks, and compromise a user's system.

External applications can open "javascript:" URIs in the browser, which is executed in context of the previous opened URL. This can be exploited to execute arbitrary script code in a user's browser session in context of an arbitrary site or execute arbitrary script code with escalated privileges via an external application (e.g. Flash or QuickTime).

This vulnerability affects versions up to and including 1.0.4.

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

**References:**

Original advisory:
http://www.mozilla.org/security/announce/mfsa2005-53.html

Other references:
http://secunia.com/advisories/14938/
http://secunia.com/advisories/16043/

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

**CVE Reference:** CAN-2005-2260, CAN-2005-2261, CAN-2005-2262, CAN-2005-2263, CAN-2005-2264, CAN-2005-2265, CAN-2005-2267, CAN-2005-2269, CAN-2005-2270

### ❖ 15667 Mozilla Property Manipulation Cross-Site Scripting Vulnerability (Remote File Checking)

Secunia Research has discovered a vulnerability in Mozilla Suite, which can be exploited by malicious people to conduct cross-site scripting attacks.

The problem is that the "frames", "parent", "self", and "top" DHTML properties are not properly protected from being modified by another site via JavaScript. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary site, which calls a method in one of the modified properties.

The vulnerability has been confirmed in version 1.7.8. Prior versions may also be affected.

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

**References:**

Original advisory:
http://secunia.com/secunia_research/2005-15/advisory/

Other references:
http://secunia.com/advisories/15551/
http://secunia.com/advisories/15549/

Product HomePage:
http://www.mozilla.org/products/mozilla1.x/

**CVE Reference:** CAN-2005-2266

### ❖ 15668 Mozilla Thunderbird DHTML properties are not properly protected Vulnerability (Remote File Checking)

Some vulnerabilities have been reported in Thunderbird, which can be exploited by malicious people to bypass certain security restrictions, gain knowledge of potentially sensitive information, conduct cross-site scripting attacks and compromise a user's system.

An error where certain DHTML properties are not properly protected from being modified can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

Versions up to and including version 1.0.4 are vulnerable.

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

**References:**

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-52.html

Other references:
http://secunia.com/advisories/16062/

http://secunia.com/advisories/14820/
http://secunia.com/advisories/15549/

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

**CVE Reference:** CAN-2005-0989, CAN-2005-1159, CAN-2005-1160, CAN-2005-2261, CAN-2005-2265, CAN-2005-2266, CAN-2005-2269, CAN-2005-2270

### ❖ 15669 Mozilla Thunderbird "InstallVersion.compareTo()" function Vulnerability (Remote File Checking)

Some vulnerabilities have been reported in Thunderbird, which can be exploited by malicious people to bypass certain security restrictions, gain knowledge of potentially sensitive information, conduct cross-site scripting attacks and compromise a user's system.

An input validation error in the handling of unexpected JavaScript objects passed to the "InstallVersion.compareTo()" function may be exploited to execute arbitrary code.

Versions up to and including version 1.0.4 are vulnerable.

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

**References:**

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-50.html

Other references:
http://secunia.com/advisories/16062/
http://secunia.com/advisories/14820/
http://secunia.com/advisories/15549/

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

**CVE Reference:** CAN-2005-0989, CAN-2005-1159, CAN-2005-1160, CAN-2005-2261, CAN-2005-2265, CAN-2005-2266, CAN-2005-2269, CAN-2005-2270

### ❖ 15670 Mozilla Thunderbird handling of DOM node names Vulnerability (Remote File Checking)

Some vulnerabilities have been reported in Thunderbird, which can be exploited by malicious people to bypass certain security restrictions, gain knowledge of potentially sensitive information, conduct cross-site scripting attacks and compromise a user's system.

An error in the handling of DOM node names with different namespaces can be exploited to execute arbitrary script code with escalated privileges via a specially crafted XHTML document.

Successful exploitation allows execution of arbitrary code.

Versions up to and including version 1.0.4 are vulnerable.

Test Case Impact: **xxxxxxxx** Vulnerability Impact: **xxxxxx** Risk: **xxxxxx**

**References:**

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-55.html

Other references:
http://secunia.com/advisories/16062/
http://secunia.com/advisories/14820/
http://secunia.com/advisories/15549/

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

**CVE Reference:** CAN-2005-0989, CAN-2005-1159, CAN-2005-1160, CAN-2005-2261, CAN-2005-2265, CAN-2005-2266, CAN-2005-2269, CAN-2005-2270

# New Vulnerabilities found this Week

- **Cisco IOS IPv6 Packet Handling Vulnerability**

"Denial of Service"

A vulnerability has been reported in Ciso IOS, which can be exploited by malicious people to cause a DoS (Denial of Service) or potentially compromise a vulnerable network device.

The vulnerability is caused due to an unspecified error within the processing of IPv6 traffic and can be exploited via a specially crafted IPv6 packet received on a logical interface.

Successful exploitation requires that the packet is sent from a local network segment and that the device is configured for IPv6.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml
http://www.kb.cert.org/vuls/id/930892

- **Debian apt-cacher Unspecified Arbitrary Command Execution**

"Execute arbitrary commands"

Eduard Bloch has reported a vulnerability in apt-cacher, which potentially can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an unspecified input validation error in the

caching system, which can be exploited to execute arbitrary commands.

References:
http://www.debian.org/security/2005/dsa-772

- **UnZip File Permissions Change Vulnerability**

"Perform certain actions on a vulnerable system with escalated privileges"

Imran Ghory has reported a vulnerability in unzip, which can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges.

The vulnerability is caused due a race condition that exists when the uncompressed file is closed and before its permissions are changed. This can be exploited via hardlink attacks to change the permissions of other files belonging to the user running unzip.

Successful exploitation requires that the malicious user is able to delete the uncompressed file and replace it with a hardlink to another file owned by the unzip user, before permissions are set on the file.

The vulnerability has been reported in version 5.52. Prior versions may also be affected.

References:
http://secunia.com/advisories/16309/

- **Microsoft ActiveSync Denial of Service and Equipment ID Enumeration**

"Denial of Service"

Seth Fogie has reported two vulnerabilities in Microsoft ActiveSync, which can be exploited by malicious people to cause a DoS (Denial of Service) and enumerate valid equipment IDs.

1) It is possible to enumerate valid equipment IDs by examining the response via some specially crafted data sent to port 5679/tcp.

This can further be exploited to trick users into disclosing passwords for mobile devices to malicious people.

2) An error in the communication handling can be exploited to freeze the ActiveSync process by sending multiple initialization requests to port 5679/tcp.

The vulnerabilities have been reported in version 3.7.1. Other versions may also be affected.

References:
http://www.airscanner.com/security/activesync371.htm

- **MySQL Eventum Cross-Site Scripting and SQL Injection**
  "Cross-site scripting and SQL injection attacks"

James Bercegay has reported some vulnerabilities in MySQL Eventum, which can be exploited by malicious people to conduct cross-site scripting and SQL injection attacks.

1) Input passed to the "id" parameter in "view.php", the "release" parameter in "list.php", and the "F" parameter in "get_jsrs_data.php" is not properly sanitised before being returned to users. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

2) Certain input passed to the release, report, and authentication classes is not properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

The vulnerabilities have been reported in versions 1.5.5 and prior.

References:
http://www.gulftech.org/?node=research&article_id=00093-07312005

- **jabberd "jid.c" Buffer Overflow Vulnerabilities**
  "Crash the server or potentially execute arbitrary code."

Michael has reported some vulnerabilities in jabberd, which potentially can be exploited by malicious users to compromise a vulnerable system.

The vulnerabilities are caused due to three boundary errors in jid.c when parsing JID strings with overly long user, host, or resource components. This can be exploited to crash the server or potentially execute arbitrary code.

References:
http://j2.openaether.org/bugzilla/show_bug.cgi?id=99

- **Trillian Exposure of User Credentials**
  "Gain knowledge of sensitive information"

Suramya Tomar has discovered a security issue in Trillian, which can be exploited by malicious, local users to gain knowledge of sensitive information.

The problem is that user credentials for Yahoo! mail accounts are stored in a world-readable HTML document inside the "users\default\cache" directory in the installation directory.

The security issue has been confirmed in Trillian Basic 3.1 (build 121) and has also been reported in versions 3.0 and 3.1 (Basic/Pro). Other versions may also

be affected.

References:
http://secunia.com/advisories/16289/

- **Linksys WRT54G Router Common SSL Private Key Disclosure**
  "Gain knowledge of certain sensitive information"

Nick Simicich has reported a security issue in WRT54G, which potentially can be exploited by malicious people to gain knowledge of certain sensitive information.

The security issue is caused due to all routers being loaded with the same certificate and SSL private key. A user with knowledge with the private key can potentially decrypt router management traffic captured from the network.

References:
http://secunia.com/advisories/16271/

**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