netVigilance

ScoutNews Team

April 29, 2005
Issue # 30

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Turn that Honeypot into a Moneypot, 'time to go long on encryption? Applications newest target for hackers and ISS security specialist goes over to the 'Dark Side'.

Enjoy reading and stay safe.

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

Top Security News Stories this Week

- **Make those Honeypots pay**

3Com announced as part of it's recent acquisition of Tipping Point; that they will begin paying security researchers for zero-day vulnerabilities.

The Zero Day Initiative (ZDI) mimics the program that was started by iDefense some years ago. With the acquisition of iDefense earlier this month by VeriSign, this puts 3Com and VeriSign in somewhat of a bidding war for Zero Day identifications and give hackers some honest work.

DataMonitor

Full Story:
http://www.computerwire.com/industries/research/?pid=A2675322-C16E-413A-88AA-5FA16A859CA4

❖ Cryptography next big thing in Security?

According to nCipher, the next great leap in security will be cryptography. The future may bring encrypted transmissions between internal servers, clients and databases.
IT-Observer

Editors note: If this is true, cryptography could yield the next 'killer-app' that spurs large-scale investment in high performance server hardware.

Full Story :
http://www.ebcvg.com/articles.php?id=814

❖ Application vulnerabilities becoming hacker's preferred targets

Hackers have apparently adopted a 'hit-em where they ain't' campaign to circumvent advances in OS security, according to the SANS Institute. By shifting their focus to popular applications such as iTunes and RealPlayer; hackers are exploiting the unaware and non-unified application vendors and hopping right over the latest advances in OS security.

This has actually caused a sharp increase in the number of vulnerabilities reported by SANS; computer vulnerabilities in the second quarter of 2005 increased 10.8 percent compared with the first quarter.
Washington Post

Related Links:
http://news.yahoo.com/news?tmpl=story&u=/washpost/20050726/tc_washpost/hackers_skip_windows_to_embed_new_infections

http://www.newsfactor.com/news/Security-Vulnerabilities-on-the-Rise/story.xhtml?story_id=12100BSB8KIH

❖ Cisco, ISS attempt to silence whistleblower

"The force is strong in this one." – Ed.

Cisco and ISS made several attempts to prevent a recent employee of ISS from giving talk on Cisco IOS vulnerabilities that allow a hacker to shut down Cisco routers running IOS through remote execution. Although Mike Lynn has lost his job at ISS and faces legal action from Cisco, he went forth with is talk at the recent Blackhats conference outlining serious flaws in Cisco's IOS allowing hackers to potentially 'shutdown the internet'.

Related Links:
http://www.securityfocus.com/news/11259

http://www.vnunet.com/vnunet/news/2140510/cisco-iss-sue-security

http://www.redherring.com/Article.aspx?a=12952&hed=TechSpin%3A+Speaker+Trumps+Cisco&sector=Industries&subsector=Communications

New Vulnerabilities Tested in SecureScout

- **16014 ProFTPD format string error shutdown message Vulnerability**

ProFTPD is an FTP server available for many Unix platforms.

A vulnerability has been reported in ProFTPD, which can be exploited by malicious users to disclose certain sensitive information, cause a DoS (Denial of Service), or potentially compromise a vulnerable system.

A format string error exists when displaying a shutdown message containing the name of the current directory. This can be exploited by a user, who creates a directory containing format specifiers and sets the directory as the current directory, when the shutdown message is being sent.

Successful exploitation requires a shutdown message containing the "%C", "%R", or "%U" variables.

The vulnerability has been fixed in version 1.3.0rc2.

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

References:

Original Advisory:
http://www.proftpd.org/docs/RELEASE_NOTES-1.3.0rc2

Other references:
http://secunia.com/advisories/16181/

Product page:
http://www.proftpd.net/

CVE Reference: CAN-2005-2390

- **16015 ProFTPD format string error response messages Vulnerability**

ProFTPD is an FTP server available for many Unix platforms.

A vulnerability has been reported in ProFTPD, which can be exploited by malicious users to disclose certain sensitive information, cause a DoS (Denial of Service), or potentially compromise a vulnerable system.

A format string error exists when displaying response messages to the client using information retrieved from a database using mod_sql. This can be exploited by a user, who inserts format string sequences into database tables that are used to generate the response messages.

Successful exploitation requires that the "SQLShowInfo" directive is set and also requires the user to have control over the contents of the used tables in the database.

The vulnerability has been fixed in version 1.3.0rc2.

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

References:

Original Advisory:

http://www.proftpd.org/docs/RELEASE_NOTES-1.3.0rc2

Other references:
http://secunia.com/advisories/16181/

Product page:
http://www.proftpd.net/

CVE Reference: CAN-2005-2390

❖ **13270 Oracle Database Server - iSQL*Plus component Unspecified error (jul-2005/DB09)**

An unspecified error in the iSQL*Plus 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

❖ **13271 Oracle Database Server - Single Sign-On component Unspecified error (jul-2005/DB10)**

An unspecified error in the Single Sign-On 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

❖ **15225 Ethereal multitude Protocol Dissectors Vulnerabilities (Remote File Checking)**

Multiple vulnerabilities have been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

Various types of errors including NULL pointer dereference errors, format string errors, infinite loop errors, and boundary errors exists in a multitude of protocol dissectors.

Successful exploitation causes Ethereal to stop responding, consume a large amount of system resources, crash, or execute arbitrary code.

The vulnerabilities affect versions 0.8.5 through 0.10.11

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00020.html

Other references:
http://secunia.com/advisories/16225/
http://secunia.com/advisories/15949/
http://secunia.com/advisories/16137/

Product:
http://www.ethereal.com/

CVE Reference: CAN-2005-2365, CAN-2005-2367

❖ **15226 Ethereal zlib library Vulnerabilitiy (Remote File Checking)**

A vulnerability has been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

Ethereal Windows installer ships with a vulnerable version of zlib library.

Successful exploitation causes Ethereal to stop responding, consume a large amount of system resources, crash, or execute arbitrary code.

The vulnerabilities affect versions 0.8.5 through 0.10.11

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00020.html

Other references:
http://secunia.com/advisories/16225/
http://secunia.com/advisories/15949/
http://secunia.com/advisories/16137/

Product:
http://www.ethereal.com/

CVE Reference: CAN-2005-2365, CAN-2005-2367

❖ **15655 AOL Instant Messenger %s 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.

The version of AOL Instant Messenger that is shipped with Netscape is subject to a denial of service. By transferring a file consisting of an unusual number of '%s' to a remote user running Windows NT or 2000, AOL Instant Messenger will crash when attempting to reveal the filename in the Instant Messenger window. A restart of the application is required in order to gain normal functionality.
Example filename: %s%s%s%s%s%s%s%s%s%s%s.jpg

Successful exploitation of this vulnerability will lead to complete comprimise of the target host.

Vulnerable: AOL Instant Messenger 4.1.2010

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

References:

Original advisory:
http://www.securityfocus.com/bid/1747

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

CVE Reference: CVE-2000-1000

❖ 15656 AOL Instant Messenger Path Disclosure 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.

If a user transmits a file through AOL Instant Messenger, the full local path of the file is displayed to the remote recipient. This information could possibly be used in order to discover the Operating System platform and other sensitive details which may assist in a future attack.

Vulnerable: AOL Instant Messenger 4.0

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

References:

Original advisory:
http://www.securityfocus.com/bid/1180

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

CVE Reference: CAN-2000-0383

❖ 15660 Firefox "InstallTrigger.install()" 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 error, where the callback function of the "InstallTrigger.install()" function is not properly cleared before navigating to a new site, can be exploited to execute arbitrary script code in a user's browser session in context of an arbitrary site.

Successful exploitation requires that the malicious web site has been added to the install whitelist.

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/mfsa2005-48.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

❖ **15661 Firefox handling of "data:" 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.

An error in the handling of "data:" URIs originating from the sidebar can be exploited to execute arbitrary script code in a user's browser session in context of an arbitrary site.

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/mfsa2005-49.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

New Vulnerabilities found this Week

❖ **Opera Download Dialog Spoofing Vulnerability**
"Trick users into executing malicious files"

Secunia Research has discovered a vulnerability in Opera, which can be exploited by malicious people to trick users into executing malicious files.

The vulnerability is caused due to an error in the handling of extended ASCII codes in the download dialog. This can be exploited to spoof the file extension in the file download dialog via a specially crafted "Content-Disposition" HTTP header.

Successful exploitation may result in users being tricked into executing a malicious file via the download dialog, but requires that the "Arial Unicode MS" font (ARIALUNI.TTF) has been installed on the system.

NOTE: The "Arial Unicode MS" font is installed with various Microsoft Office distributions.

The vulnerability has been confirmed in version 8.01. Other versions may also be affected.

References:
http://secunia.com/advisories/15870/

- **Opera Image Dragging Vulnerability**
  "Conduct cross-site scripting attacks and retrieve a user's files"

  Secunia Research has discovered a vulnerability in Opera, which can be exploited by malicious people to conduct cross-site scripting attacks and retrieve a user's files.

  The vulnerability is caused due to Opera allowing a user to drag e.g. an image, which is actually a "javascript:" URI, resulting in cross-site scripting if dropped over another site. This may also be used to populate a file upload form, resulting in uploading of arbitrary files to a malicious web site.

  Successful exploitation requires that the user is tricked into dragging and dropping e.g. an image or a link.

  The vulnerability has been confirmed in version 8.01. Prior versions may also be affected.

  References:
  http://secunia.com/advisories/15756/

- **Ethereal Multiple Protocol Dissector and zlib Vulnerabilities**
  "Denial of Service"

  Multiple vulnerabilities have been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

  1) Various types of errors including NULL pointer dereference errors, format string errors, infinite loop errors, and boundary errors exists in a multitude of protocol dissectors.

  2) Ethereal Windows installer ships with a vulnerable version of zlib library.

Successful exploitation causes Ethereal to stop responding, consume a large amount of system resources, crash, or execute arbitrary code.

The vulnerabilities affect versions 0.8.5 through 0.10.11

References:
http://www.ethereal.com/appnotes/enpa-sa-00020.html
http://secunia.com/advisories/16225/

- **Vim Modelines Shell Command Execution Vulnerability**
  "Execute shell commands when the user opens a specially crafted file"

  Georgi Guninski has reported a vulnerability in vim, which can be exploited by malicious people to compromise a vulnerable system.

  The vulnerability is caused due to an error that allows the "glob()" command to be exploited to execute shell commands when the user opens a specially crafted file.

  Successful exploitation allows command execution with privileges of the vim user, but requires the "modelines" option to be enabled and the user is tricked into opening a malicious file.

  The vulnerability has been reported in versions prior to 6.3.082.

  References:
  http://www.guninski.com/where_do_you_want_billg_to_go_today_5.html

- **GroupWise Client Buffer Overflow Vulnerability**
  "Denial of Service"

  Francisco Amato has reported a vulnerability in GroupWise Client, which can be exploited by malicious, local users to cause a DoS (Denial of Service) or potentially gain escalated privileges.

  The vulnerability is caused due a boundary error in the client when parsing the file containing the labels of different views (i.e. GWVW02??.INI). This can be exploited to cause a buffer overflow when the client attempts to log into the post office.

  Successful exploitation requires permissions to modify the GWVW02??.INI files, which is normally restricted to administrative users.

  The vulnerability has been reported in version 6.5.

  References:
  http://support.novell.com/cgi-bin/search/searchtid.cgi?/10098314.htm
  http://www.infobyte.com.ar/adv/ISR-12.html

- **ProFTPD Two Format String Vulnerabilities**
  "Disclose certain sensitive information; cause a DoS (Denial of Service)"

  Two vulnerabilities have been reported in ProFTPD, which can be exploited by malicious users to disclose certain sensitive information, cause a DoS (Denial of Service), or potentially compromise a vulnerable system.

  1) A format string error exists when displaying a shutdown message containing the name of the current directory. This can be exploited by a user, who creates a directory containing format specifiers and sets the directory as the current directory, when the shutdown message is being sent.

  Successful exploitation requires a shutdown message containing the "%C", "%R", or "%U" variables.

  2) A format string error exists when displaying response messages to the client using information retrieved from a database using mod_sql. This can be exploited by a user, who inserts format string sequences into database tables that are used to generate the response messages.

  Successful exploitation requires that the "SQLShowInfo" directive is set and also requires the user to have control over the contents of the used tables in the database.

  References:
  http://www.proftpd.org/docs/RELEASE_NOTES-1.3.0rc2

- **Apache HTTP Request Smuggling Vulnerability**
  "Conduct HTTP request smuggling attacks"

  A vulnerability has been reported in Apache, which can be exploited by malicious people to conduct HTTP request smuggling attacks.

  The vulnerability is caused due to an error in the handling of malformed HTTP requests with both "Transfer-Encoding" and "Content-Length" headers and can be exploited to cause Apache to forward malicious HTTP requests in the HTTP body, which will be processed as a separate HTTP requests by the receiving server.

  Successful exploitation allows poisoning of the web proxy cache or bypass of certain web application firewall protections, but requires that Apache is configured as a web proxy.

  An off-by-one error has also been reported in mod_ssl when printing debug information and configured to use a malicious CRL (Certificate

Revocation List).

References:
http://secunia.com/advisories/14530/

- **MySQL Multiple Vulnerabilities**
  "Denial of Service"

  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.

  1) MySQL uses a vulnerable version of the zlib library.

  2) It is possible for malicious users to crash the server in various ways. See the vendor advisory for details.

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

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