netVigilance

ScoutNews Team **July 8, 2005**
Issue # 27

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Microsoft UK site defaced, Sophos PC survival numbers are out, IM vulnerabilities becoming a serious concern for business and large retailer gets hit hard for loosing credit card data.

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

- **Microsoft UK hacked in defacing attack**

A hacker in the UK posted a gif image and a message in apparent support of jailed hacker Rafa. This appears to be really an act of vandalism against a soft web server.
The Register

Full Story :
http://www.theregister.com/2005/07/06/msuk_hacked/

- **Sophos releases new report on survival time for PCs**

Although the Sophos data is somewhat more pessimistic that previously released number from the Internet Storm Center, it still is a strong indicator of the ever-decreasing time

window that an unprotected PC could be connected to the internet before getting infected.

The lesson is still the same: install a firewall, anti-virus and conduct a vulnerability scan before you venture out onto the web.

TechWeb News

Related Links:
http://www.crn.com/sections/breakingnews/breakingnews.jhtml?articleId=165700440

- **IM threats Mushrooming**

The IMlogic Threat Center reports a 2,747 percent increase in new IM threats for the 1st quarter of 2005. In an interesting development, over 70% of the reported incidents were from enterprises and small businesses

InfoWorld

Related Links:
http://www.infoworld.com/article/05/07/08/28OPsecadvise_1.html

- **Retailer gets heavy penalty for loss of customer information**

After falling victim to a hacker attack where they lost customer's credit card information, BJ's Wholesale Club settled charges from the Federal Trade Commission, agreeing to submit to outside security audits for 20 years and to tighten protection of customer information.

They are also facing about $13 million in private claims as a result of the loss of data. Credit card fraud already costs the retail industry an estimated $1.5 Billion per year.

InformationWeek

Full Story:
http://www.informationweek.com/story/showArticle.jhtml;jsessionid=WRCDQPK1C0V4GQSNDBGCKH0CJUMEKJVN?articleID=165600216&tid=6004

New Vulnerabilities Tested in SecureScout

- **13253 Golden FTP Server Pro Information Disclosure Weakness (Remote File Checking)**

Lachlan. H has discovered a weakness in Golden FTP Server Pro, which can be exploited by malicious users to gain knowledge of various information.

An input validation error in the handling of the LS command makes it possible to disclose the contents of the application directory (e.g. containing files with names of valid users) by changing directory to a share and then pass "\.." as argument to the LS command.

The weakness has been confirmed in version 2.60.
Other versions may also be affected.

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

References:

Original Advisories:
http://secunia.com/advisories/15840/

Product HomePage:
http://www.goldenftpserver.com/

CVE Reference: None

❖ **13254 Golden FTP Server Pro absolute path Information Disclosure Weakness (Remote File Checking)**

Lachlan. H has discovered a weakness in Golden FTP Server Pro, which can be exploited by malicious users to gain knowledge of various information.

It's possible to disclose the absolute path of a share by changing directory to it and then attempt to retrieve a non-existing file.

The weakness has been confirmed in version 2.60.
Other versions may also be affected.

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

References:

Original Advisories:
http://secunia.com/advisories/15840/

Product HomePage:
http://www.goldenftpserver.com/

CVE Reference: None

❖ **13255 Golden FTP Server Pro Directory Traversal Vulnerability (Remote File Checking)**

Lachlan. H has reported a vulnerability in Golden FTP Server Pro, which can be exploited by malicious users to access arbitrary files on a vulnerable system.

The vulnerability is caused due to an input validation error making it possible to escape the FTP root and retrieve or place arbitrary files on the system via directory traversal attacks using the "\.." character sequence.

It is also possible to disclose the absolute path of the FTP root by attempting to retrieve a non-existent file.

The vulnerability has been reported in version 2.52. Other versions may also be affected.

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

References:

Original Advisories:
http://secunia.com/advisories/15175/

Product HomePage:
http://www.goldenftpserver.com/

CVE Reference: CAN-2005-1484, CAN-2005-1485

❖ **13256 Golden FTP Server Pro Log Parsing Buffer Overflow Vulnerability (Remote File Checking)**

Reed Arvin has reported a vulnerability in Golden FTP Server Pro, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the log parsing functionality when handling entries in the "gftppro.log" log file. This can e.g. be exploited to cause a stack-based buffer overflow by passing an overly long argument (about 336 bytes) to the "USER" FTP command when attempting to log in.

Successful exploitation allows execution of arbitrary code, but either requires that an administrative user afterwards attempts to view the statistics or the FTP server is restarted. Also, to regain normal functionality if the FTP server crashes, the malicious entry in the "gftppro.log" file has to be removed manually.

The vulnerability has been confirmed in version 2.52. Other versions may also be affected.

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

References:

Original Advisories:
http://secunia.com/advisories/15156/

Product HomePage:
http://www.goldenftpserver.com/

CVE Reference: None

❖ **13257 Golden FTP Server Pro "RNTO" Command Buffer Overflow (Remote File Checking)**

barabas mutsonline has reported a vulnerability in Golden FTP Server Pro, which can be exploited by malicious users to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the handling of the "RNTO" FTP command. This can be exploited to cause a buffer overflow by supplying an overly long argument.

Successful exploitation may allow execution of arbitrary code.

Not vulnerable version: 2.05b.

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

References:

Original Advisories:
http://secunia.com/advisories/13966/

Other references:
http://www.kb.cert.org/vuls/id/620862

Product HomePage:
http://www.goldenftpserver.com/

CVE Reference: CAN-2005-0566

❖ **13258 Golden FTP Server Pro Information Disclosure Weakness (FTP)**

Lachlan. H has discovered a weakness in Golden FTP Server Pro, which can be exploited by malicious users to gain knowledge of various information.

An input validation error in the handling of the LS command makes it possible to disclose the contents of the application directory (e.g. containing files with names of valid users) by changing directory to a share and then pass ".." as argument to the LS command.

The weakness has been confirmed in version 2.60.
Other versions may also be affected.

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

References:

Original Advisories:
http://secunia.com/advisories/15840/

Product HomePage:
http://www.goldenftpserver.com/

CVE Reference: None

❖ **13259 Golden FTP Server Pro absolute path Information Disclosure Weakness (FTP)**

Lachlan. H has discovered a weakness in Golden FTP Server Pro, which can be exploited by malicious users to gain knowledge of various information.

It's possible to disclose the absolute path of a share by changing directory to it and then attempt to retrieve a non-existing file.

The weakness has been confirmed in version 2.60.
Other versions may also be affected.

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

References:

Original Advisories:
http://secunia.com/advisories/15840/

Product HomePage:
http://www.goldenftpserver.com/

CVE Reference: None

❖ **13260 Golden FTP Server Pro Directory Traversal Vulnerability (FTP)**

Lachlan. H has reported a vulnerability in Golden FTP Server Pro, which can be exploited by malicious users to access arbitrary files on a vulnerable system.

The vulnerability is caused due to an input validation error making it possible to escape the FTP root and retrieve or place arbitrary files on the system via directory traversal attacks using the ".." character sequence.

It is also possible to disclose the absolute path of the FTP root by attempting to retrieve a non-existent file.

The vulnerability has been reported in version 2.52. Other versions may also be affected.

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

References:

Original Advisories:
http://secunia.com/advisories/15175/

Product HomePage:
http://www.goldenftpserver.com/

CVE Reference: CAN-2005-1484, CAN-2005-1485

❖ 13261 Golden FTP Server Pro Log Parsing Buffer Overflow Vulnerability (FTP)

Reed Arvin has reported a vulnerability in Golden FTP Server Pro, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the log parsing functionality when handling entries in the "gftppro.log" log file. This can e.g. be exploited to cause a stack-based buffer overflow by passing an overly long argument (about 336 bytes) to the "USER" FTP command when attempting to log in.

Successful exploitation allows execution of arbitrary code, but either requires that an administrative user afterwards attempts to view the statistics or the FTP server is restarted. Also, to regain normal functionality if the FTP server crashes, the malicious entry in the "gftppro.log" file has to be removed manually.

The vulnerability has been confirmed in version 2.52. Other versions may also be affected.

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

References:

Original Advisories:
http://secunia.com/advisories/15156/

Product HomePage:
http://www.goldenftpserver.com/

CVE Reference: None

❖ 13262 Golden FTP Server Pro "RNTO" Command Buffer Overflow (FTP)

barabas mutsonline has reported a vulnerability in Golden FTP Server Pro, which can be exploited by malicious users to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the handling of the "RNTO" FTP command. This can be exploited to cause a buffer overflow by supplying an overly long argument.

Successful exploitation may allow execution of arbitrary code.

Not vulnerable version: 2.05b.

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

References:

Original Advisories:
http://secunia.com/advisories/13966/

Other references:
http://www.kb.cert.org/vuls/id/620862

Product HomePage:
http://www.goldenftpserver.com/

CVE Reference: CAN-2005-0566

New Vulnerabilities found this Week

- **Internet Explorer "javaprxy.dll" Memory Corruption Vulnerability**
  "Execution of arbitrary code"

  SEC Consult has discovered a vulnerability in Microsoft Internet Explorer, which can be exploited by malicious people to compromise a user's system.

  The vulnerability is caused due to the javaprxy.dll COM object being instantiated incorrectly in Internet Explorer via the object tag. This can be exploited via a malicious web site to cause a memory corruption.

  Successful exploitation allows execution of arbitrary code, but requires that the file "javaprxy.dll" exists on the system.

  NOTE: "javaprxy.dll" is included with Microsoft Java Virtual Machine. Exploit code is publicly available.

  The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0, Microsoft VM (virtual machine) build 3802 and Microsoft Windows XP SP2. Internet Explorer 5.01 and 5.5 is reportedly also affected.

  References:
  http://www.microsoft.com/technet/security/advisory/903144.mspx
  http://www.sec-consult.com/184.html
  http://www.kb.cert.org/vuls/id/939605

- **Adobe Acrobat Reader UnixAppOpenFilePerform Buffer Overflow Vulnerability**
  "Execute arbitrary code"

  A vulnerability has been reported in Adobe Acrobat Reader, which potentially can be exploited by malicious people to compromise a user's system.

  The vulnerability is caused due to a boundary error in "UnixAppOpenFilePerform()" when Acrobat Reader is opening a document containing a "/Filespec" tag. This can be exploited to execute arbitrary code with the privileges of the user running Acrobat Reader by tricking the user to open a specially crafted PDF document.

The vulnerability has been reported in Adobe Acrobat Reader for Unix version 5.0.9 and 5.0.10.

References:
http://www.adobe.com/support/techdocs/329083.html
http://www.idefense.com/application/poi/display?id=279&type=vulnerabilities

❖ **zlib "inftrees.c" Buffer Overflow Vulnerability**
"Denial of Service"

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.

The vulnerability has been reported in version 1.2.2. Prior versions may also be affected.

References:
http://www.gentoo.org/security/en/glsa/glsa-200507-05.xml

❖ **GNATS Arbitrary File Overwrite Security Issue**
"Overwrite arbitrary files"

A security issue has been reported in GNATS, which can be exploited by malicious, local users to overwrite arbitrary files on a vulnerable system.

The security issue is caused due to "gen-index" being installed with suid root when compiled from sources and when the "gnat" user and group do not exist. This can be exploited by malicious users to overwrite arbitrary files by running "gen-index" with the filename to overwrite as the parameter to the "-o" argument.

The security issue has been reported in version 4.0 and 4.1.0. Prior versions might also be affected.

References:
http://www.pi3.int.pl/adv/gnats.txt

❖ **OpenLDAP / pam_ldap / nss_ldap Password Disclosure Security Issue**

"Gain knowledge of sensitive information"

A security issue has been reported in OpenLDAP, pam_ldap and nss_ldap, which can be exploit by malicious people to gain knowledge of sensitive information.

The security issue is caused due to the client not connecting to the master server using TLS when it is referred by the slave server to the master server for password changes. This allows malicious people to gain knowledge of users' password by sniffing network traffic.

The security issue has been reported in OpenLDAP version 2.2.26, pam_ldap version 1.76 and nss_ldap 2.239. Other versions may also be affected.

References:
http://bugs.gentoo.org/show_bug.cgi?id=96767

- **Golden FTP Server Pro Information Disclosure Weaknesses**

"Gain knowledge of various information"

Lachlan. H has discovered some weaknesses in Golden FTP Server Pro, which can be exploited by malicious users to gain knowledge of various information.

1) An input validation error in the handling of the LS command makes it possible to disclose the contents of the application directory (e.g. containing files with names of valid users) by changing directory to a share and then pass "\.." as argument to the LS command.

2) It's possible to disclose the absolute path of a share by changing directory to it and then attempt to retrieve a non-existing file.

The weaknesses have been confirmed in version 2.60. Other versions may also be affected.

References:
http://secunia.com/advisories/15840/

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