netVigilance

ScoutNews Team **25 December 2004**
Issue #52

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Merry Christmas,

This is the time of the year when hacking, electronic crime and vandalism spikes.

We expect 2005 to show even more malicious activity over the Internet.

Microsoft will be bringing some of its spam blocking technology out as Exchange Edge Services features into Exchange Server 2003 Service Pack 2 (SP2) that the company plans to release in the second half of 2005

Enjoy reading

Top Security News Stories this Week

- **Hackers Aim to Sabotage Holiday Computing**
  Hackers, spammers and spies go into overdrive in December and January, when unsuspecting neophytes unwrap new computers, connect to the Internet, and, too often, get hit with viruses, spyware and other nefarious programs.
  "People want to get on the Net right away, just like they want to put together and start using any Christmas present," said Tony Redmond, chief technology officer of Palo Alto, Calif.-based computer giant Hewlett-Packard Co., whose new PCs ship with 60 days of virus and adware protection. "They should be warned that the Net is a very, very dangerous place."
  http://story.news.yahoo.com/news?tmpl=story&cid=562&ncid=738&e=1&u=/ap/20041225/ap_on_hi_te/holiday_computer_hazards
  Rachel Konrad

- **Will 2005 Bring a Safer Internet?**
  Sometimes writing about security is just too easy. Making predictions about next year is like this in some ways.
  Let's pick some of the low-hanging fruit early. Even though most spam-tracking companies show that spam already comprises 75 percent or more of all e-mail, that

proportion will go up in 2005. We are approaching the situation in which, I have always assumed, users will begin to withdraw from e-mail because it is so unpleasant.
http://story.news.yahoo.com/news?tmpl=story&cid=1738&ncid=1212&e=6&u=/zd/20041224/tc_zd/141298
Larry Seltzer

- **Microsoft Backpedals on Exchange Security Roadmap**

Microsoft Corp. Wednesday disclosed that it will not ship—as a separate product—its Exchange Edge Services, a set of e-mail security and anti-spam enhancements for Exchange Server.
In May, Microsoft said it would roll out **Exchange Edge Services** in 2005. The package was expected to provide support for identification standards, such as SPF (Sender Policy Framework), as well as other tools and techniques designed to stop spam, including IP Safelist, or presolved puzzle validity—a technology that requires e-mail servers to solve complex computational puzzles for each message they send out.
http://www.eweek.com/article2/0,1759,1745123,00.asp?kc=EWRSS03119TX1K0000594
John Pallatto

New Vulnerabilities Tested in SecureScout

- **15145 ArGoSoft 1.8.x Mail Server Script Insertion Vulnerability (Remote File Checking)**

A vulnerability has been reported in ArGoSoft Mail Server, which can be exploited by malicious people to conduct script insertion attacks.

Input passed in mails is not properly sanitised before being used. This can be exploited to inject arbitrary HTML and script code, which will be executed in a user's browser session in context of an affected site when the malicious mail is viewed.

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

CVE Links:

Reference: http://www.argosoft.com/mailserver/default.aspx & http://secunia.com/advisories/13571/

- **15146 Windows XP SP2 Firewall Dial-Up Security Issue "My Network (subnet) only" (886185) (Remote File Checking)**

Some dial-up software configures the routing tables in a way that leads the Windows Firewall to determine that the whole dial-up connection is on the local subnet. After you install critical update 886185, Windows Firewall will no longer interpret network connections to be on the local subnet if they have IP Route Table entries that have an IP address of 0.0.0.0 and a mask of 0.0.0.0. This means that any port exceptions or program exceptions that use the My network (subnet) only scope option in Windows Firewall will not be available over most dial-up connections. You will still be able to access exceptions over a dial-up connection if you remove all scope restrictions or if you create a custom scope for exceptions.

Local network subnet configuration varies depending on the network that you are connected to and how that network is configured. Using the My network (subnet) only scope restriction does not guarantee security because it relies on the network subnet configuration to define what is the local network.

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

CVE Links:

Reference: http://support.microsoft.com/kb/886185 & http://www.microsoft.com/downloads/details.aspx?familyid=da66a0ac-55ca-4591-b3e6-d78695899141&displaylang=en & http://www.microsoft.com/technet/community/columns/cableguy/cg0204.mspx

- **15147 Windows Media Player 9.x ActiveX Control "getItemInfoByAtom()" Vulnerability (Remote File Checking)**

Arman Nayyeri has discovered the following vulnerability in Microsoft Windows Media Player, which can be exploited by malicious people to disclose system information, and modify or disclose some sensitive information.

An error in the "getItemInfoByAtom()" function in the Windows Media Player ActiveX control can be exploited by e.g. a malicious web site to determine the presence and size of local files.

The vulnerability has been confirmed on a fully patched system with Microsoft Windows Media Player 9 and Microsoft Windows 2000 SP4 / XP SP1 / XP SP2.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: M**edium**

CVE Links:

Reference: http://secunia.com/advisories/13578/ & http://www.microsoft.com/downloads/details.aspx?FamilyID=b446ae53-3759-40cf-80d5-cde4bbe07999&displaylang=en

- **15148 Windows Media Player 9.x ActiveX Control "setItemInfo()" and "getItemInfo()" Vulnerability (Remote File Checking)**

Arman Nayyeri has discovered the following vulnerability in Microsoft Windows Media Player, which can be exploited by malicious people to disclose system information, and modify or disclose some sensitive information.

Some errors in the "setItemInfo()" and "getItemInfo()" functions in the Windows Media Player ActiveX control can be exploited by e.g. a malicious web site to modify or disclose local media information (e.g. artist, album, and song name of a .wma file).

The vulnerability has been confirmed on a fully patched system with Microsoft Windows Media Player 9 and Microsoft Windows 2000 SP4 / XP SP1 / XP SP2.

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

CVE Link:

Reference: http://secunia.com/advisories/13578/ & http://www.microsoft.com/downloads/details.aspx?FamilyID=b446ae53-3759-40cf-80d5-cde4bbe07999&displaylang=en

- **15149 WinRAR Delete File Buffer Overflow Vulnerability (Remote File Checking)**

Vafa Khoshaein has discovered a vulnerability in WinRAR.

The vulnerability is caused due to a boundary error in the handling of filenames when deleting files in archives. This can be exploited to cause a buffer overflow by tricking a user into deleting a file in an opened, malicious archive.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been confirmed on versions 3.40 and 3.41. Other versions may also be affected.

Test Case Impact: **Gather info** Vulnerability Impact: **Attack** Risk: **Medium**

CVE Link: CAN-2004-1254

Reference: http://secunia.com/advisories/13591/ & http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1254 & http://www.rarlabs.com/download.htm

- **15150 WinRAR Directory Traversal Vulnerability (Remote File Checking)**

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

The vulnerability has been reported in version 3.20 and is similar to a known vulnerability in UnZip.

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

CVE Link:

Reference: http://secunia.com/advisories/9790/ & http://www.rarlabs.com/download.htm

- **15151 WinRAR buffer overflow Vulnerability (Remote File Checking)**

WinRAR does not handle long filenames correctly, by supplying a long file extension (more than 256 characters) a buffer overflow is caused, this is exploitable and could allow malicious people to execute arbitrary code with the privileges of the logged in user.

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

CVE Link:

Reference: http://secunia.com/advisories/7933/ & http://www.rarlabs.com/download.htm

- **15614 ArGoSoft 1.8.x Mail Server Script Insertion Vulnerability (SMTP Check)**

A vulnerability has been reported in ArGoSoft Mail Server, which can be exploited by malicious people to conduct script insertion attacks.

Input passed in mails is not properly sanitised before being used. This can be exploited to inject arbitrary HTML and script code, which will be executed in a user's browser session in context of an affected site when the malicious mail is viewed.

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

CVE Link:

Reference: http://www.argosoft.com/mailserver/default.aspx & http://secunia.com/advisories/13571/

- **17930 Apache 2 Memory consumption DoS**

Apache webserver 2.0.52 and earlier allows remote attackers to cause a denial of service (CPU consumption) via an HTTP GET request with a MIME header containing multiple lines with a large number of space characters.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS** Risk: **High**

CVE Link: CAN-2004-0942

Reference: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0942 & http://www.apacheweek.com/features/security-20

- **15554 Cisco CatOS Embedded HTTP Server Buffer Overflow (CSCdy26428)**

Cisco Catalyst switches running specific versions of Cisco CatOS software are vulnerable to a buffer overflow in an embedded HTTP server.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS** Risk: **High**

CVE Link: CAN-2002-1222

Reference:http://www.cisco.com/en/US/products/products_security_advisory09186a00800fd774.shtml

New Vulnerabilities found this Week

- **Rpm Finder "web()" Buffer Overflow and Insecure File Creation**

“Perform certain actions with escalated privileges”
Two vulnerabilities have been reported in Rpm Finder, which can be exploited by malicious people to compromise a user's system and by malicious, local users to perform certain actions with escalated privileges.
1) A boundary error in the "web()" function when handling data from a remote server can be exploited to cause a stack-based buffer overflow by tricking a user into connecting to a malicious web server.
2) Insecure creation of files can be exploited via symlink attacks to truncate arbitrary files with the privileges of the user running rpf.
The vulnerabilities have been reported in version 1.2.2. Other versions may also be affected.
References:

http://www.rosiello.org/en/read_projects.php?id=2

❖ **Debian debmake Insecure Temporary Directory Creation**

"Overwrite arbitrary files"

Javier Fernández-Sanguino Peña has reported a vulnerability in debmake, 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 debstd script creating temporary directories insecurely. This can be exploited via symlink attacks to overwrite arbitrary files with the privileges of the user running the vulnerable script.

References:

http://www.debian.org/security/2004/dsa-615

❖ **Citrix Metaframe XP Unspecified Buffer Overflow Vulnerability**

"Execution of arbitrary code"

A vulnerability has been reported in Citrix Metaframe XP, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an unspecified boundary error, which can be exploited to cause a buffer overflow.

Successful exploitation may allow execution of arbitrary code.

References:

http://support.citrix.com/kb/entry.jspa?externalID=CTX104982#P28_3724w

❖ **Linux Kernel Multiple Vulnerabilities**

"Denial of Service; Gain knowledge of potentially sensitive information**"**

Multiple vulnerabilities have been reported in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service) or gain knowledge of potentially sensitive information.

1) A NULL pointer dereference error in the "aio_free_ring()" system call can be exploited to crash the system by mapping out as much of the process address space as possible and then call the "io_setup()" function with an extremely large value (about 65000) in the "nr_events" argument.

The vulnerability has been reported in version 2.6.9. Other versions may also be affected.

2) An error in the DRM (Direct Rendering Manager) drivers due to insufficient DMA lock checking can be exploited to crash the X server or modify video output.

3) A race condition within the handling of "/proc/…/cmdline" may disclose the content of environment variables of spawning processes.

❖ **WinRAR Delete File Buffer Overflow Vulnerability**

"Execution of arbitrary code"

Vafa Khoshaein has discovered a vulnerability in WinRAR, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the handling of filenames when deleting files in archives. This can be exploited to cause a buffer overflow by tricking a user into deleting a file in an opened, malicious archive.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been confirmed on versions 3.40 and 3.41. Other versions may also be affected.

❖ **LibTIFF Two Integer Overflow Vulnerabilities**

"Execute arbitrary code"

infamous41md has reported two vulnerabilities in LibTIFF, which can be exploited by malicious people to compromise a vulnerable system.

1) The vulnerability is caused due to an integer overflow in the "TIFFFetchStripThing()" function in "tif_dirread.c" when parsing TIFF files. This can be exploited via a specially crafted TIFF image file to execute arbitrary code via an application linked against the vulnerable library.

The vulnerability has been reported in version 3.6.1. Other versions may also be affected.

2) The vulnerability is caused due to an integer overflow in the "CheckMalloc()" function in "tif_dirread.c" and "tif_fax3.c" when handling data from a certain directory entry in the file header. This can be exploited via specially crafted TIFF image file to execute arbitrary code via an application linked against the vulnerable library.

The vulnerability has been reported in versions 3.5.7 and 3.7.0. Other versions may also be affected.

References:

http://www.idefense.com/application/poi/display?id=173&type=vulnerabilities

http://www.idefense.com/application/poi/display?id=174&type=vulnerabilities

❖ **HP-UX FTP Server Debug Logging Buffer Overflow Vulnerability**

"Execution of arbitrary code"

iDEFENSE has reported a vulnerability in HP-UX, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the debug logging routine of ftpd. This can be exploited to cause a stack-based buffer overflow by sending a specially crafted, overly long command request.

Successful exploitation may allow execution of arbitrary code, but requires that the FTP daemon is configured to log debug information (not default setting).

References:

http://www.idefense.com/application/poi/display?id=175&type=vulnerabilities

❖ **Google Desktop Search Exposure of Local Search Results**

"View local search results"

A vulnerability has been reported in Google Desktop Search, which can be exploited by malicious people to view local search results.

The problem is that it is possible for Java applets (and possibly JavaScript and other plug-ins) to trigger fake Google searches that will cause Google Desktop Search to return local results, which normally would be embedded in search results from Google. These results can then be read by the Java applet and sent back to a malicious web site.

Successful exploitation requires that a user is tricked into visiting a malicious web site.

Versions prior to 121004 are vulnerable.

References:

http://seclab.cs.rice.edu/

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