netVigilance

**ScoutNews Team** **January 14th 2005**
**Issue # 2**

Weekly ScoutNews by netVigilance

**Table of Contents**

This Week in Review
Top Security News Stories this Week
New Test Cases Tested in SecureScout
New Vulnerabilities this Week

# This Week in Review

The ever increasing connectivity of cell phones and PDAs is fast becoming a vulnerable target for the people on the dark side.
With the lack of speed our society demonstrates in responding to both digital and physical security threats it is safe to judge we will be further behind a year from now. FBI has used $170M tax money on a system that is obsolete when being implemented.
Authorities are still chasing spammers, but why is it not stopping?

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

- **Secret Service Data Compromised in T-Mobile Hack**
  A malicious hacker penetrated the network of mobile phone company T-Mobile USA and accessed information on 400 of the company's customers, including sensitive information from the account of a U.S. Secret Service agent, according to statements by T-Mobile and the Secret Service.
  http://story.news.yahoo.com/news?tmpl=story&ncid=1293&e=3&u=/pcworld/20050114/tc_pcworld/119318&sid=95612664
  Paul Roberts

- **FBI May Have to Scrap New Computer Program**
  The FBI said on Thursday it may have to scrap a new $170 million computer program designed to allow agents to share information instantly and fix a main problem identified after the Sept. 11 attacks.
  The software is already outdated and inadequate, with the bureau able to use only about one-tenth of the program, an FBI official said on condition of anonymity.
  Failure of the Virtual Case File software is the latest glitch in the bureau's effort to overhaul its computer system, one of FBI Director Robert Mueller's priorities in the

agency's reorganization after the Sept. 11, 2001, attacks.
http://story.news.yahoo.com/news?tmpl=story&ncid=1209&e=8&u=/nm/20050114/tc_nm/security_software_dc&sid=95573713
Reuters

- **Texas AG Sues Student Over Spamming**

The state attorney general filed a lawsuit against a 22-year-old college student and his business partner, accusing them of illegally sending hundreds of thousands of unsolicited, misleading e-mails.
Ryan Pitylak, a student at the University of Texas at Austin, heads the fourth-largest spamming operation in the world, Attorney General Gregg Abbott said.
The lawsuit filed Thursday alleges Pitylak, with Mark Trotter, his 40-year-old business partner in California, have been sending the e-mails since at least Sept. 1, 2003.
http://story.news.yahoo.com/news?tmpl=story&cid=562&e=2&u=/ap/spam_lawsuit
Brandi Grissom

# New Vulnerabilities Tested in SecureScout

- **14681 Vulnerability in HTML Help Could Allow Code Execution (MS05-001/890175) (Remote File Checking)**

A vulnerability exists in the HTML Help ActiveX control in Windows that could allow information disclosure or remote code execution on an affected system.

If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system could be less impacted than users who operate with administrative privileges.

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

**CVE Links:** CAN-2004-1043

**Reference:** http://www.microsoft.com/technet/security/Bulletin/MS05-001.mspx & http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1043 & http://archives.neohapsis.com/archives/bugtraq/2004-12/0426.html

- **14682 Vulnerability in Cursor and Icon Format Handling Could Allow Remote Code Execution (MS05-002/891711) (Remote File Checking)**

A remote code execution vulnerability exists in the way that cursor, animated cursor, and icon formats are handled. An attacker could try to exploit the vulnerability by constructing a malicious cursor or icon file that could potentially allow remote code execution if a user visited a malicious Web site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A denial of service vulnerability exists in the way that cursor, animated cursor, and icon formats are handled. An attacker could try to exploit the vulnerability by constructing a malicious cursor or icon file that could potentially cause the operating system to become

unresponsive. The operating system would have to be restarted to restore functionality.

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

**CVE Links:** CAN-2004-1049 & CAN-2004-1305

**Reference:** http://www.microsoft.com/technet/Security/bulletin/ms05-002.mspx & http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1049 & http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1305

- **14683 Vulnerability in the Indexing Service Could Allow Remote Code Execution (MS05-003/871250) (Remote File Checking)**

A remote code execution vulnerability exists in the Indexing Service because of the way that it handles query validation. An attacker could exploit the vulnerability by constructing a malicious query that could potentially allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take complete control of an affected system. While remote code execution is possible, an attack would most likely result in a denial of service condition.

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

**CVE Links:** CAN-2004-0897

**Reference:** http://www.microsoft.com/technet/security/bulletin/MS05-003.mspx & http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0897

- **14684 Mozilla Dialog Overlapping Weakness (Remote File Checking)**

mikx has discovered a weakness in Mozilla which potentially can be exploited by malicious people to trick users into performing unintended actions.

The problem is that popup windows can overlay modal dialogs. This can e.g. be exploited by a malicious web site to hide the information text in a download or security dialog in order to trick a user into accepting it.

Exploitation is more or less convincing depending on the used Windows desktop theme.

The issue is beeing addressed in Mozilla 1.7.6.

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

**CVE Link:**

**Reference:** http://www.mikx.de/?p=7 & http://www.mozilla.org/projects/security/known-vulnerabilities.html & http://www.mozilla.org/products/mozilla1.x/

- **15154 Winamp Unspecified "in_cdda.dll" Buffer Overflow Vulnerability (Remote File Checking)**

A vulnerability with an unknown impact has been reported in Winamp.

The vulnerability is reportedly caused due to an error in in_cdda.dll and can be exploited

to cause a buffer overflow.

This vulnerability has been addressed in Winamp version 5.08c.

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

**CVE Link:**

**Reference:** http://www.winamp.com/ & http://forums.winamp.com/showthread.php?s=&threadid=202799 & http://www.security-assessment.com/Papers/Winamp_IN_CDDA_Buffer_Overflow.pdf

- **15569 SNMP System Contact Disclosure**

SNMP is a network protocol used for network management.
Wrong configuration could lead to the disclosure of information like the system administrator of the host.
This information could be used for social engineering.

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

**CVE Link:**

**Reference:** http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm & http://en.wikipedia.org/wiki/Simple_network_management_protocol

- **15570 SNMP System Hardware Disclosure**

SNMP is a network protocol used for network management.
Wrong configuration could lead to the disclosure of information such as the host's system model and manufacturer.
This information could be used for further attacks against the host.

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

**CVE Link:**

**Reference:** http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm & http://en.wikipedia.org/wiki/Simple_network_management_protocol

- **15571 SNMP System Uptime Disclosure**

SNMP is a network protocol used for network management.
Wrong configuration could lead to the disclosure of information such as the host's uptime.
This information could be used for identifying the host maintenance level.

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

**CVE Link:**

**Reference:** http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm & http://en.wikipedia.org/wiki/Simple_network_management_protocol

- **15572 SNMP System Name Disclosure**

SNMP is a network protocol used for network management.
Wrong configuration could lead to the disclosure of information such as the host's SNMP name.
This information could be used for identifying the topology of the target network.

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

**CVE Link:** GENERIC-MAP-NOMATCH

**Reference:** http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm & http://en.wikipedia.org/wiki/Simple_network_management_protocol

- **15573 SNMP System Location Disclosure**

SNMP is a network protocol used for network management.
Wrong configuration could lead to the disclosure of information such as the host's location.
This information could be used for identifying the topology of the target network.

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

**CVE Link:** GENERIC-MAP-NOMATCH

**Reference:** http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm & http://en.wikipedia.org/wiki/Simple_network_management_protocol

# New Vulnerabilities found this Week

- **Linux Kernel Page Fault Handler Privilege Escalation**

"Gain escalated privileges"

Paul Starzetz has reported a vulnerability in the Linux kernel, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to a race condition in the page fault handler when two threads, which share the same virtual memory space, request a stack expansion simultaneously.

Successful exploitation may allow execution of arbitrary code with root privileges on multi-processor systems.

The vulnerability has been reported in versions 2.4 through 2.4.29-rc1 and 2.6 through 2.6.10.

References:
http://www.isec.pl/vulnerabilities/isec-0022-pagefault.txt
http://www.kernel.org/
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.11-rc1

- **OpenBSD TCP Retransmission Timeout Calculation Denial of Service**

"Denial of Service"

A vulnerability has been reported in OpenBSD, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the TCP stack when calculating TCP retransmission timeouts. This can be exploited to crash the system by sending some specially crafted packets with specific values in the TCP timestamp option.

References:
OpenBSD 3.6: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.6/common/010_rtt.patch
OpenBSD 3.5: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/027_rtt.patch

- **Check Point Firewall-1 NG SmartDefense RFC2397 Bypass Weakness**

"Malware to bypass detection"

A weakness has been reported in Check Point Firewall-1 NG with SmartDefense, which allows malware to bypass detection.

The weakness is caused due to a lack of RFC2397 support. This can be exploited to bypass the malware detection by sending malicious image files, which are base64 encoded and embedded in an HTML file according to the standard specified in RFC2397, which is supported by a number of client applications capable of rendering HTML files (e.g. email clients and browsers).

A PoC has been published, which embeds an image that attempts to exploit the GDI+ JPEG parsing vulnerability in Microsoft Windows.

This has been reported to affect Check Point Firewall-1 NG R55 HFA08 with SmartDefense 541041226. Other versions may also be vulnerable.

References:
http://www.intrusense.com/av-bypass/image-bypass-advisory.txt

- **Mozilla / Mozilla Firefox Dialog Overlapping Weakness**

"Hide the information text in a download or security dialog"

mikx has discovered a weakness in Mozilla and Mozilla Firefox, which potentially can be exploited by malicious people to trick users into performing unintended actions.

The problem is that popup windows can overlay modal dialogs. This can e.g. be exploited by a malicious web site to hide the information text in a download or security dialog in order to trick a user into accepting it.

Exploitation is more or less convincing depending on the used Windows desktop theme.

The weakness has been confirmed on Mozilla Firefox 1.0 and Mozilla 1.7.5 for Windows.

References:
http://www.mikx.de/?p=7

- **Winamp Unspecified "in_cdda.dll" Buffer Overflow Vulnerability**

A vulnerability with an unknown impact has been reported in Winamp.

The vulnerability is reportedly caused due to an error in in_cdda.dll and can be exploited to cause a buffer overflow.

No more information is currently available.

References:
http://forums.winamp.com/showthread.php?s=&threadid=202799

- **Linux Kernel Multiple Vulnerabilities**

"Denial of Service, disclose sensitive information, or gain escalated privileges"

Multiple vulnerabilities have been reported in the Linux kernel, which potentially can be exploited by malicious, local users to cause a DoS (Denial of Service), disclose sensitive information, or gain escalated privileges on a vulnerable system.

1) A signedness error in the "poolsize_strategy()" function of the random poolsize sysctl handler (drivers/char/random.c) can potentially be exploited to cause a buffer overflow when copying data from user space into kernel space.

Successful exploitation may crash the system or allow execution of arbitrary code with escalated privileges. However, exploitation requires UID 0, but not any root capabilities.

The vulnerability has been reported in the 2.4 and 2.6 kernel branches.

2) Two signedness errors in the "sg_scsi_ioctl()" function in "drivers/block/scsi_ioctl.c" can be exploited to cause a buffer overflow or disclose large portions of kernel memory when copying data to and from user space.

Successful exploitation may disclose sensitive information, crash the system, or potentially allow execution of arbitrary code with escalated privileges.

The vulnerabilities have been reported in the 2.6 kernel branch.

3) Boundary errors in various functions of the MOXA serial driver (drivers/char/moxa.c) can be exploited to cause buffer overflows when copying data from user space into a kernel space buffer.

Successful exploitation may allow execution of arbitrary code with escalated privileges.

The vulnerabilities have been reported in the 2.2, 2.4, and 2.6 kernel branches.

4) An unprivileged process can reportedly bypass the RLIMIT_MEMLOCK soft resource limit and lock more memory than permitted via the "mlockall()" system call.

The vulnerability has been reported in versions 2.6.9 and 2.6.10.

References:
http://www.kernel.org/
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.11-rc1

- **Squid NTLM fakeauth_auth Helper Denial of Service**

"Denial of Service"

A vulnerability have been reported in Squid, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the handling of NTLM type 3 messages in the NTLM "fakeauth_auth" helper in "fakeauth_auth.c". This can be exploited to cause a vulnerable component to crash by sending a specially crafted message.

The vulnerability has been reported in version 2.5. Other versions may also be affected.

References:
http://www.squid-cache.org/Versions/v2/2.5/bugs/#squid-2.5.STABLE7-fakeauth_auth

- **mpg123 Mpeg Layer-2 Buffer Overflow Vulnerability**

"Heap-based buffer overflow"

Yuri D'Elia has reported a vulnerability in mpg123, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error in the parsing of frame headers for layer-2 streams. This may be exploited to cause a heap-based buffer overflow via a specially crafted MP2 or MP3 file.

Successful exploitation may allow execution of arbitrary code with the privileges of the user executing mpg123.

The vulnerability has been reported in version 0.59r. Other versions may also be affected.

References:
http://security.gentoo.org/glsa/glsa-200501-14.xml

**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