ScoutNews Team **25 September 2004**
Issue #39

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

No Picture is Safe anymore, the GDI Bug discovered last week, enables hackers to gain control of your computer when you just view a JPEG picture, in a browser, email, web-mail or chat. The JPEG format is used in 75% of the pictures that you view on the Internet, and the Exploit is already among hackers. **PATCH - PATCH – PATCH !!!.** This weeks SecureScout Update will tell you if you are vulnerable. Together with earlier similar bugs in BMP and GIF, 99.5% of all pictures on the internet can now be compromised. Extortion by DDOS is gaining popularity among cybercriminals.

Enjoy reading

Top Security News Stories this Week

- **Symantec: Viruses aimed at Microsoft rise sharply**
  The number rose 400% between January and June in comparison with 2003
  The number of new viruses and worms aimed at Microsoft Corp.'s ubiquitous Windows operating system rose 400% between January and June from the same period a year earlier, computer security company Symantec Corp. said yesterday.
  Nearly 5,000 new Windows viruses and worms were documented in the first half of the year, up from about 1,000 in the same period a year earlier, said Cupertino, Calif.-based Symantec.

http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,96046,00.html?SKC=hacking-96046

Reuters

- **Credit card firm hit by DDoS attack**
  Credit card processing firm Authorize.Net has been the target of an "intermittent" and "large scale" distributed denial-of-service attack since last Wednesday that has resulted in "periodic disruptions" of service for some customers.
  http://www.computerworld.com/securitytopics/security/story/0,10801,96099,00.html?SKC=security-96099

Jaikumar Vijayan

- **Microsoft Lists XP SP2 Problems**
  Microsoft has released a long list of programs that are affected by its new XP SP 2 patch, including many of its own products, and security experts are counseling companies to

take a wary approach to using the update. "Don't apply it until you know that it's working," says Secunia CTO Thomas Kristensen.

http://www.newsfactor.com/story.xhtml?story_title=Microsoft_Lists_XP_SP__Problems&story_id=26344#story-start

To see the list of affected programs click here :
http://support.microsoft.com/default.aspx?kbid=842242&product=windowsxpsp2

Kimberly Hill

- **TruSecure, Betrusted to merge and rename**
  Security companies TruSecure and Betrusted are expected to formally announce on Tuesday that they plan to merge and create a newly formed company called Cybertrust. Consultancy TruSecure will be joined by Betrusted, which, through various acquisitions, has grown to focus on three security segments: public key infrastructure, security consulting services and managed security services such as monitoring firewalls.
  http://news.com.com/Security+firms+TruSecure+and+Betrusted+to+merge/2100-7350_3-5374949.html

Dawn Kawamoto

New Vulnerabilities Tested in SecureScout

- **14658 Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (MS04-028/833987) (Remote File Checking)**
  A buffer overrun vulnerability exists in the processing of JPEG image formats that could allow remote code execution on an affected system.

  If a user is logged on with administrator privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

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

CVE Links: CAN-2004-0200

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-028.mspx

- **15080 Vulnerability in WordPerfect Converter Could Allow Code Execution (MS04-027/884933) (Remote File Checking)**
  A remote code execution vulnerability exists in the WordPerfect 5.x Converter that is provided as part of the affected software.

  If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges. However, user interaction is required to exploit this vulnerability.

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

CVE Links: CAN-2004-0573

Reference: http://www.microsoft.com/technet/security/bulletin/ms04-027.mspx

❖ 13173 ICQ Installed (Remote File Checking)

The remote host is using ICQ - a p2p software,
which may not be suitable for a business environment.

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

CVE Links: CAN-1999-1418, CAN-1999-1440, CAN-2000-0046, CAN-2000-0564, CVE-2000-0552, CAN-2001-0367, CVE-2002-0028, CAN-2001-1305

Reference: http://www.icq.com/, http://www.securityfocus.com/bid/1307,
http://www.securityfocus.com/bid/132, http://www.securityfocus.com/bid/246,
http://www.securityfocus.com/bid/2664, http://www.securityfocus.com/bid/3226,
http://www.securityfocus.com/bid/3813, http://www.securityfocus.com/bid/929

❖ 15088 Trillian Installed (Remote File Checking)

The remote host is using Trillian - a p2p software,
which may not be suitable for a business environment

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.trillian.cc/
Bugtraq:
http://www.securityfocus.com/bid/5677
http://www.securityfocus.com/bid/5733
http://www.securityfocus.com/bid/5733
http://www.securityfocus.com/bid/5765
http://www.securityfocus.com/bid/5769
http://www.securityfocus.com/bid/5776
http://www.securityfocus.com/bid/5777
http://www.securityfocus.com/bid/5783

❖ 15094 Yahoo! Messenger IMVironment XSS Vulnerability (Remote File Checking)

Yahoo! Messenger is a free instant messaging software.

Yahoo Messenger contains a flaw that allows a remote Cross Site Scripting attack. This flaw exists because the application does not validate a "ymsgr:" URI that specifies an invalid IMVironment. This could allow an attacker to execute arbitrary HTML or script code on a user's client. Such an attack could disclose a user's Yahoo ID and encoded password.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: Vendor URL: http://messenger.yahoo.com/
Bugtraq: http://www.securityfocus.com/bid/9158

❖ 15128 Yahoo! Audio Conferencing ActiveX Control Overflow Vulnerability (Remote File Checking)

Yahoo! Messenger is a free instant messaging software.

Yahoo! Audio Conferencing contains a flaw that may allow a remote attacker to execute arbitrary code. The issue is due to an unchecked buffer in the Audio Conferencing ActiveX Control. If an attacker sends a specially crafted request, they may be able to overflow the buffer and execute arbitrary code.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: Vendor URL: http://messenger.yahoo.com/
Vendor Advisory URL: http://help.yahoo.com/help/us/mesg/use/use-45.html
Bugtraq: http://www.securityfocus.com/bid/7561

❖ 15129 Trillian AIM Overflow (Remote File Checking)

The remote host is using Trillian - a p2p software,
which may not be suitable for a business environment.

A bug has been reported in the AOL Instant Messenger (AIM) portion of Trillian. A remote attacker, exploiting this flaw, would be potentially able to execute code on the client system running Trillian.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.trillian.cc/
http://security.e-matters.de/advisories/022004.html

❖ 15130 Yahoo! Messenger yauto.dll Overflow Vulnerability (Remote File Checking)

Yahoo! Messenger is a free instant messaging software.

YAUTO.DLL is an ActiveX/COM component that comes with Yahoo Messenger. YAUTO.DLL is registered under a ProgID called "YAuto.NSAuto.1". Since this is an ActiveX component, the vulnerability can be exploited just by making a website with the correct CLSID of the ActiveX and call the function directly. The author reports successfully exploiting the vulnerability by creating a website that can download a trojan and execute it silently.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: Vendor URL: http://messenger.yahoo.com/
Vendor Advisory URL: http://messenger.yahoo.com/security/update4.html
http://lists.netsys.com/pipermail/full-disclosure/2003-December/014434.html

- **15286 Trillian MSN Overflow (Remote File Checking)**

  The remote host is using Trillian - a p2p software,
  which may not be suitable for a business environment.

  A bug has been reported in the AOL Instant Messenger (AIM) portion of Trillian. A remote attacker, exploiting this flaw, would be potentially able to execute code on the client system running Trillian.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.trillian.cc/
http://www.securityfocus.com/bid/11142

- **15131 Winamp Skin File Local Zone Arbitrary Code Execution Vulnerability (Remote File Checking)**

  The Winamp Player is a flexible and sophisticated application for playing and managing music.

  WinAmp contains a flaw that may allow a malicious user to execute arbitrary code. The issue is triggered when a user downloads a specifically crafted WinAmp skin from a malicious website. These skins are downloaded without prompting the user when using Internet Explorer. It is possible that the flaw may allow an attacker to to place and execute arbitrary programs resulting in a loss of confidentiality, integrity, or availability.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: Vendor URL: http://www.winamp.com/
Advisory URL: http://k-otik.com/exploits/08252004.skinhead.php
Generic Exploit URL: http://k-otik.com/exploits/08252004.skinhead.rar

New Vulnerabilities found this Week

- **Symantec Firewall/VPN Products Multiple Vulnerabilities**

"Denial of Service; identify active services; and manipulate the firewall configuration"

Rigel Kent Security & Advisory Services has reported some vulnerabilities in various Symantec Firewall/VPN products, which can be exploited by malicious people to cause a

DoS (Denial of Service), identify active services, and manipulate the firewall configuration.

1) An error within the connection handling can be exploited to cause the firewall to stop responding via a UDP port scan of all ports on the WAN interface.

This vulnerability affects the following products:
* Symantec Firewall/VPN Appliance 100 (firmware builds prior to build 1.63)
* Symantec Firewall/VPN Appliance 200/200R (firmware builds prior to build 1.63)

2) An access control error in the default firewall ruleset causes any incoming UDP traffic from port 53 to be accepted. This makes it possible for a malicious person to port scan a system for listening UDP services on the WAN interface and communicate with these by using port 53/udp as source port.

This vulnerability affect the following products:
* Symantec Firewall/VPN Appliance 100 (firmware builds prior to build 1.63)
* Symantec Firewall/VPN Appliance 200/200R (firmware builds prior to build 1.63)
* Symantec Gateway Security 320 (firmware builds prior to build 622)
* Symantec Gateway Security 360/360R (firmware builds prior to build 622)

3) The default SNMP read/write community strings can't be changed nor can the SNMP service be disabled. This can be exploited in combination with vulnerability #2 to disclose and manipulate the firewall configuration via the SNMP service.

This vulnerability affect the following products:
* Symantec Firewall/VPN Appliance 100 (firmware builds prior to build 1.63)
* Symantec Firewall/VPN Appliance 200/200R (firmware builds prior to build 1.63)
* Symantec Gateway Security 320 (firmware builds prior to build 622)
* Symantec Gateway Security 360/360R (firmware builds prior to build 622)

References: http://www.sarc.com/avcenter/security/Content/2004.09.22.html

❖ **ColdFusion MX Sensitive Information Disclosure and Denial of Service**
“Denial of Service”

Two vulnerabilities have been reported in ColdFusion MX Server, which can be exploited by malicious people to disclose sensitive information and cause a DoS (Denial of Service).

References: http://www.macromedia.com/devnet/security/security_zone/mpsb04-09.html

❖ **OpenBSD Radius Authentication "login_radius" Security Bypass**
“Bypass certain security restrictions”

Eilko Bos has reported a vulnerability in OpenBSD, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to "login_radius" not checking the shared secret on replies from the radius server. This can be exploited by sending a specially crafted, spoofed response

with the origin of the radius server.

Successful exploitation requires that radius authentication is enabled (not enabled by default).

References:

ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/020_radius.patch

ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.4/common/031_radius.patch

- **xine-lib Multiple Buffer Overflow Vulnerabilities**

  "Stack-based buffer overflow"

Multiple vulnerabilities have been reported in xine-lib, which can be exploited by malicious people to compromise a user's system.

1) A boundary error within the VideoCD functionality when reading ISO disk labels can be exploited to cause a stack-based buffer overflow by passing an overly long disk label.

2) A boundary error within the handling of text subtitles can be exploited to cause a buffer overflow and may allow arbitrary code execution via a specially crafted file.

3) A boundary error within the DVD subpicture decoder can be exploited to cause a heap-based buffer overflow. This may allow execution of arbitrary code via e.g. a malicious MPEG file.

References: http://xinehq.de/index.php/releases

- **Sun Java Enterprise System NSS Library Vulnerability**

  "Compromise a vulnerable system"

Sun has acknowledged a vulnerability in the NSS library included with Sun Java Enterprise System, which can be exploited by malicious people to compromise a vulnerable system.

References: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57643-1

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