netVigilance

ScoutNews Team **April 1, 2005**
Issue # 13

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

netVigilance has completed the move to larger office space, an ISP in the UK gets extremely high catch rate on Spam cost effective solution, stating the obvious; Cyber crime is on the rise, Symantec admits to new AV holes and [white] hats off to FBI Infragard, attention to cyber crime drives digital forensics education.

Good reading

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

Top Security News Stories this Week

- **netVigilance moves into new, larger quarters**

Although the pool and the espresso machine will be dearly missed, we are extremely happy to have finished the move to our new larger workspace; trading our cheek-to-jowl existence for the luxury of larger and more private offices.

Our new mailing address is:

17937 SW McEwan Rd.
Suite 250
Portland, OR 97224-7768

- **UK ISP implements easy / effective Spam filtering using Spamhaus block lists.**

By deploying a 2-stage filtering methodology; uxn.com, a UK based ISP, achieves a catch rate of 99.6% with zero false positives.

The process uses Spamhaus filters on the first stage and an application that can scan incoming messages for Spamhaus Block List (SBL) urls on the 2nd stage.

I like this solution, it appears to be simple and low-cost.
The Spamhaus Project

Read more Here :
http://www.spamhaus.org/effective_filtering.html

- **Cyber crime on the rise; increase in weak broadband fostering Botnet attacks.**

That's right, Botnets; 'herds' of computers pressed into service to launch DoS, spam and Phishing. Organized crime gangs may be behind this new wave bent on collecting banking and identity credentials.

ZDNet UK

Full Story:
http://news.zdnet.co.uk/0,39020330,39193449,00.htm

- **Symantec discloses 2 new vulnerabilities in AV products.**

Norton Anti-Virus products contain 2 holes allowing DoS attacks against users of the software. Vulnerabilities are listed as 'Low' threat lever since they have not been associated with any major customer outages.

A trend that is becoming more and more common, this announcement highlights the importance of deploying overlapping security measures and keeping all security products updated and installed.

IDG News Service

Full Story:
http://www.nwfusion.com/news/2005/0330symanackno.html

- **Center of Excellence in Digital Forensics at Sam Houston State University, ready to open in the fall.**

Dr. David Burris, a professor of computer science at Sam Houston attributes the increase in awareness directly to the Infragard program. With well publicized hacks to Federal government and the increasing cost of hacker damage, there is a shortage of talented digital forensics specialists.

Full Story:
http://www.infragard.net/press_room/articles/article_030305.htm

New Vulnerabilities Tested in SecureScout

- **15179 Java Web Start JNLP File Command Line Argument Injection Vulnerability (Remote File Checking)**

Jouko Pynnönen has reported a vulnerability in Java Web Start, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an input validation error when handling property tags in JNLP files. This can be exploited to pass arbitrary command line arguments to the virtual machine by tricking a user into opening a malicious JNLP file.

Successful exploitation can lead to the Java "sandbox" being disabled.

NOTE: JNLP files are opened automatically in Microsoft Internet Explorer.

The vulnerability affects Java Web Start included in J2SE releases 1.4.2 through 1.4.2_06 for Windows, Solaris and Linux.

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

References:

Original Advisory:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57740-1
http://jouko.iki.fi/adv/ws.html

Other References:
http://www.securityfocus.com/bid/12847
http://secunia.com/advisories/14640/

Product HomePage:

http://java.sun.com/j2se/

CVE Reference: CAN-2005-0836

❖ 15494 IMail IMAP Service DELETE Command Buffer Overflow Vulnerability

Muts has discovered a vulnerability in IMail Server, which can be exploited by malicious users to compromise a vulnerable system.

The vulnerability is caused due to a boundary error within the IMAP service ("IMAP4D32.exe") when processing "DELETE" commands. This can be exploited to cause a stack-based buffer overflow by passing a "DELETE" command with an overly long argument (about 300 bytes).

Successful exploitation allows execution of arbitrary code.

The vulnerability has been confirmed in version 8.13. Other versions may also be affected.

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

References:

Initial Advisory :
http://www.ipswitch.com/Support/ICS/updates/im814hf1.html

Vendor:
http://www.ipswitch.com/Products/IMail_Server/index.html

CVE Reference: CAN-2004-1520

❖ 15495 IMail IMAP Service EXAMINE Buffer Overflow Vulnerability

Nico Steinhardt has reported a vulnerability in Ipswitch Collaboration Suite, which can be exploited by malicious users to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the IMAP4 service (IMAP4d32.exe) shipped with IMail Server, which is now part of Ipswitch Collaboration Suite. This can be exploited to cause a buffer overflow by passing an overly long string (about 259 bytes) as argument to the "EXAMINE" command.

Successful exploitation allows execution of arbitrary code.

The vulnerability has been reported in IMAP4d32.exe version 12.8.27.14

(included in IMail Server 8.13). Other versions may also be affected.

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

References:

Initial Advisory :
http://www.idefense.com/application/poi/display?id=216&type=vulnerabilities

Other references:
http://secunia.com/advisories/14546/

Vendor:
http://www.ipswitch.com/Products/IMail_Server/index.html

CVE Reference: CAN-2005-0707

- **15584 Trillian Multiple buffer overflows Vulnerabilities (Remote File Checking)**

LogicLibrary has reported some vulnerabilities in Trillian, allowing malicious people to compromise a users system.

The vulnerabilities are caused due to boundary errors in the handling of HTTP/1.1 response headers. This can be exploited to cause a heap-based buffer overflow and execute arbitrary code by sending a maliciously crafted HTTP/1.1 response.

Successful exploitation requires that the attacker controls a server, which Trillian connects to, or is able to conduct a Man-in-the-Middle attack.

The vulnerabilities have been reported in the AIM, MSN, RSS and possibly other plug-ins in Trillian 2.0. It has also been reported in the Yahoo IM and possibly other plug-ins in Trillian version 3.0 and 3.1.

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

References:

http://www.trillian.cc/
http://marc.theaimsgroup.com/?l=bugtraq&m=111171416802350&w=2
http://secunia.com/advisories/14689

CVE Reference: CAN-2005-0874

- **15585 Trillian Yahoo plug-in buffer overflows Vulnerabilities (Remote File Checking)**

Multiple buffer overflows in the Yahoo plug-in for Trillian 2.0, 3.0, and 3.1 allow remote web servers to cause a denial of service (application crash) via a long string in an HTTP 1.1 response header.

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

References:

http://www.trillian.cc/
http://marc.theaimsgroup.com/?l=bugtraq&m=111171416802350&w=2
http://secunia.com/advisories/14689

CVE Reference: CAN-2005-0875

- **15586 Opera IDN Spoofing Security Issue (Remote File Checking)**

Eric Johanson has reported a security issue in Opera, which can be exploited by a malicious web site to spoof the URL displayed in the address bar, SSL certificate, and status bar.

The problem is caused due to an unintended result of the IDN (International Domain Name) implementation, which allows using international characters in domain names.

This can be exploited by registering domain names with certain international characters that resembles other commonly used characters, thereby causing the user to believe they are on a trusted site.

The issue has been confirmed in Opera versions 7.54u1 and 7.54u2. Other versions may also be affected.

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

References:

Original advisory:
http://www.shmoo.com/idn/homograph.txt

Other References:
http://www.cs.technion.ac.il/~gabr/papers/homograph.html
http://www.icann.org/committees/idn/idn-codepoint-paper.htm

CVE Reference: CAN-2005-0235

- **15587 Opera "data:" URI Handler Spoofing Vulnerability (Remote File Checking)**

Michael Holzt 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 processing of "data:" URIs, causing wrong information to be shown in a download dialog. This can be exploited by e.g. a malicious website to trick users into executing a malicious file by supplying a specially crafted "data:" URI.

The vulnerability has been confirmed on version 7.54u1 for Windows. Other versions may also be affected.

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

References:

Original advisory:
http://www.kb.cert.org/vuls/id/882926

Other References:
http://secunia.com/advisories/13818/

CVE Reference: CAN-2005-0456

- **15588 Opera Download Dialog Spoofing Vulnerability (Remote File Checking)**

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 the filename and the "Content-Type" header not being sufficiently validated before being displayed in the file download dialog. This can be exploited to spoof file types in the download dialog by passing specially crafted "Content-Disposition" and "Content-Type" headers containing dots and ASCII character code 160.

Successful exploitation may result in users being tricked into executing a malicious file via the download dialog.

The vulnerability has been confirmed on Opera 7.54 for Windows. Other versions may also be affected.

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

References:

Original advisory:
http://secunia.com/secunia_research/2004-19/advisory/

Other References:
http://www.opera.com/support/search/supsearch.dml?index=782

CVE Reference: CAN-2004-1490

❖ 15589 Opera Window Injection Vulnerability (Remote File Checking)

Secunia Research has reported a vulnerability in Opera, which can be exploited by malicious people to spoof the content of websites.

The problem is that a website can inject content into another site's window if the target name of the window is known. This can e.g. be exploited by a malicious website to spoof the content of a pop-up window opened on a trusted website.

The vulnerability has been confirmed in Opera version 7.54. Other versions may also be affected.

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

References:

Original advisory:
http://secunia.com/secunia_research/2004-13/advisory/
http://www.opera.com/support/search/supsearch.dml?index=782

Other References:
http://secunia.com/advisories/11978/

CVE Reference: CAN-2004-1157

❖ 15590 Opera "sun.*" System Information Disclosure Weakness (Remote File Checking)

Marc Schoenefeld has reported a weakness in Opera, which can be exploited by malicious people to disclose some system information.

Opera accesses the JRE (Java Runtime Environment) directly instead of using the Java plugin. The problem is that the "accessClassInPackage" permission is improperly given to the "sun.*" packages, which can be exploited by a malicious untrusted applet to gain knowledge of the full path to the currently logged in user's username and installation directory.

Successful exploitation requires that Sun Java is installed and that the

permission "accessClassInPackage sun.*" is given in "Opera.policy" (default).

The weakness has been reported in version 7.54. Other versions may also be affected.

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

References:

http://secunia.com/advisories/13257/

CVE Reference: none.

New Vulnerabilities found this Week

- **Cisco VPN Concentrator 3000 Series HTTPS Packet Denial of Service**
  "Denial of Service"

  A vulnerability has been reported in Cisco VPN Concentrator 3000 Series, which can be exploited by malicious people to cause a DoS (Denial of Service).

  The vulnerability is caused due to an unspecified error within the SSL handling and can be exploited to cause a vulnerable device to reload and/or drop user connections by sending specially crafted HTTPS packets to the device.

  Successful exploitation requires that the HTTPS service is enabled (not enabled by default) and can be accessed by the malicious person.

  The vulnerability affects devices running software version 4.1.7.A and prior.

  References:
  http://www.cisco.com/warp/public/707/cisco-sa-20050330-vpn3k.shtml

- **GTK+ BMP Loader Double Free Denial of Service Vulnerability**
  "crash certain applications on a user's system"

  David Costanzo has reported a vulnerability in GTK+, which can be exploited by malicious people to crash certain applications on a user's system.

  The vulnerability is caused due to a double free error in the BMP loader. This can be exploited to crash an application linked against GTK+ when a specially crafted BMP image is processed.

References:
http://secunia.com/advisories/14775/

- **Kerio Personal Firewall Network Rules Security Bypass**
  "bypass the firewall rules"

  Petr Matousek has reported a vulnerability in Kerio Personal Firewall, which can be exploited by malicious programs to bypass the firewall rules.

  The vulnerability is caused due to an error making it possible for a malicious process to bypass the firewall network rules by impersonating another process allowed to access the Internet.

  Successful exploitation requires that a malicious program has been executed on the user's system.

  The vulnerability affects versions 4.1.2 and prior.

  References:
  http://www.kerio.com/security_advisory.html#0503

- **Sun Solaris Telnet Client Buffer Overflow Vulnerabilities**
  "Buffer Overflow"

  Gaël Delalleau has reported two vulnerabilities in the telnet client included with Sun Solaris, which can be exploited by malicious people to compromise a vulnerable system.

  References:
  http://sunsolve.sun.com/search/document.do?assetkey=1-26-57755-1
  http://www.idefense.com/application/poi/display?id=220&type=vulnerabilities
  http://www.idefense.com/application/poi/display?id=221&type=vulnerabilities

- **Symantec Norton AntiVirus Denial of Service Vulnerabilities**
  "Denial of Service"

  Isamu Noguchi has reported two vulnerabilities in Symantec Norton AntiVirus, which can be exploited by malicious people to cause a DoS (Denial of Service).

  1) An unspecified error in the Auto-Protect module during scan of specific file types can be exploited to cause the system to hang or crash.

  2) An error in the SmartScan feature in Auto-Protect, when a file located

on a network share is renamed, can be exploited to consume a large amount of CPU resources or cause a system crash.

The following products are affected:
* Symantec Norton AntiVirus 2004
* Symantec Norton Internet Security 2004 (Professional)
* Symantec Norton SystemWorks 2004 (Professional)
* Symantec Norton AntiVirus 2005
* Symantec Norton Internet Security 2005
* Symantec Norton SystemWorks 2005 (Premier)

References:
http://securityresponse.symantec.com/avcenter/security/Content/2005.03.28.html

❖ **Linux Kernel Multiple Vulnerabilities**
"Denial of Service"

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

1) Some unspecified errors have been reported in the ISO9660 filesystem handler including Rock Ridge and Juliet extensions. These can be exploited via a specially crafted filesystem to cause a DoS or potentially corrupt memory leading to execution of arbitrary code.

2) A signedness error in the "bluez_sock_create()" function when creating bluetooth sockets can potentially be exploited to gain root privileges on a vulnerable system.

3) An information leak exists in ext2 when creating new directories and may disclose kernel memory.

4) An error in load_elf_library can be exploited to cause a DoS.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.6
http://kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.30.log

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