netVigilance

**ScoutNews Team** **October 28, 2005**
**Issue # 43**

Weekly ScoutNews by netVigilance

**Table of Contents**



## This Week in Review

US universities get 'F' in network security, Zotob makes big cleanup impact and watch out for bird flu virus via email.

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

- **Universities failing network security**

Citing lack of funding and staff, a CDW survey of 100 colleges and universities in the US; shows that they are lagging on network security and are acutely aware of this.

Only five percent of the schools surveyed said that they are very safe from attack.
CRN

Full Story :
http://www.eschoolnews.com/news/showStoryts.cfm?ArticleID=5923

- **Zotob; small but costly**

The Zotob variant that hit in august was limited in its spread turned out to be very costly

for those that did get infected.

The companies that reported getting infected by the worm said that it took 80 hours of work to recover. In the survey conducted by CyberTrust, 700 companies were interviewed with average costs running about $97,000

Redherring

Related Links:
http://www.redherring.com/Article.aspx?a=14206&hed=Zotob+Cost+%2497K+per+Company&sector=Industries&subsector=SecurityAndDefense

- **Bird flu Trojan snares word users**

Using topical subject lines in email seems to be the method of choice for Phishing scammers. In the latest, the case of the newly discovered Trojan horse, dubbed "Navia.a".

The email has been seen with the subjects: "Outbreak in North America" and "What is avian influenza (bird flu)?" Users are baited into opening a word document which installs malicious macros that change, create and delete files. It then installs another Trojan that opens a back-door into the PC.

TechWeb News

Related Links:
http://www.informationweek.com/story/showArticle.jhtml?articleID=172900962
http://www.esecurityplanet.com/trends/article.php/3559321

# New Vulnerabilities Tested in SecureScout

- **13299 Skype "skype://" URI Handler Buffer Overflow Vulnerability (Remote File Checking)**

  Skype is a free program that uses the latest P2P (cutting edge p2p technology) technology to bring affordable and high-quality voice communications to Some vulnerabilities have been reported in Skype, which can be exploited by malicious people to cause a DoS or to compromise a user's system.

  A boundary error exists when handling Skype-specific URI types e.g. "callto://" and "skype://". This can be exploited to cause a buffer overflow and allows arbitrary code execution when the user clicks on a specially-crafted Skype-specific URL.

  Successful exploitation may allow execution of arbitrary code.

  Vulnerability has been reported in Skype for Windows Release 1.1.*.0 through 1.4.*.8

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

**References:**

Original advisories:
http://www.skype.com/security/skype-sb-2005-02.html
http://www.skype.com/security/skype-sb-2005-03.html
http://www.pentest.co.uk/documents/ptl-2005-01.html

Other references:
http://secunia.com/advisories/13191/
http://www.kb.cert.org/vuls/id/668193
http://www.kb.cert.org/vuls/id/905177
http://www.kb.cert.org/vuls/id/930345

Product Home Page:
http://www.skype.com/

**CVE Reference:** CVE-2005-3265, CVE-2005-3267

### ❖ 13300 Skype "unicode_to_bytes()" Buffer Overflow Vulnerability (Remote File Checking)

Skype is a free program that uses the latest P2P (cutting edge p2p technology) technology to bring affordable and high-quality voice communications to Some vulnerabilities have been reported in Skype, which can be exploited by malicious people to cause a DoS or to compromise a user's system.

A boundary error exists in the handling of VCARD imports. This can be exploited to cause a buffer overflow and allows arbitrary code execution when the user imports a specially-crafted VCARD.

Vulnerability has been reported in Skype for Windows Release 1.1.*.0 through 1.4.*.83.

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

**References:**

Original advisories:
http://www.skype.com/security/skype-sb-2005-02.html
http://www.skype.com/security/skype-sb-2005-03.html
http://www.pentest.co.uk/documents/ptl-2005-01.html

Other references:
http://secunia.com/advisories/13191/
http://www.kb.cert.org/vuls/id/668193
http://www.kb.cert.org/vuls/id/905177
http://www.kb.cert.org/vuls/id/930345

Product Home Page:
http://www.skype.com/

**CVE Reference:** CVE-2005-3265, CVE-2005-3267

### ❖ 13301 Skype integer overflow via specially-crafted UDP packet Vulnerability (Remote File Checking)

Skype is a free program that uses the latest P2P (cutting edge p2p technology) technology to bring affordable and high-quality voice communications to Some vulnerabilities have been reported in Skype, which can be exploited by malicious people to cause a DoS or to compromise a user's system.

An integer overflow error exists when allocating memory in response to certain received Skype client network UDP packet. This can be exploited to cause a heap-based buffer overflow via a specially-crafted UDP packet.

Successful exploitation crashes the Skype client. It has been reported that the vulnerability is also exploitable via TCP and allows arbitrary code execution via overwritten function pointers on the heap.

Vulnerability has been reported in Skype for Windows Release 1.1.*.0 through 1.4.*.83.

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

**References:**

Original advisories:
http://www.skype.com/security/skype-sb-2005-02.html
http://www.skype.com/security/skype-sb-2005-03.html
http://www.pentest.co.uk/documents/ptl-2005-01.html

Other references:
http://secunia.com/advisories/13191/
http://www.kb.cert.org/vuls/id/668193
http://www.kb.cert.org/vuls/id/905177
http://www.kb.cert.org/vuls/id/930345

Product Home Page:
http://www.skype.com/

**CVE Reference:** CVE-2005-3265, CVE-2005-3267

### ❖ 13302 Oracle Database Server - Materialized Views component Unspecified error (oct-2005/DB11)

An unspecified error in the Materialized Views component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

**References:**

Original Advisory:

http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

Product Homepage:
http://www.oracle.com/

**CVE Reference:** CAN-2005-0873

### ❖ 13303 Oracle Database Server - Materialized Views component Unspecified error (oct-2005/DB12)

An unspecified error in the Materialized Views component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

**References:**

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

Product Homepage:
http://www.oracle.com/

**CVE Reference:** CAN-2005-0873

### ❖ 13304 Oracle Database Server - Objects Extension component Unspecified error (oct-2005/DB13)

An unspecified error in the Objects Extension component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

**References:**

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

Product Homepage:
http://www.oracle.com/

**CVE Reference:** CAN-2005-0873

### ❖ 13305 Oracle Database Server - Oracle Intelligent Agent component Unspecified error (oct-2005/DB14)

An unspecified error in the Oracle Intelligent Agent component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

**References:**

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

Product Homepage:
http://www.oracle.com/

**CVE Reference:** CAN-2005-0873

### ❖ 15249 Ethereal NULL pointer dereference errors, divide by zero error, infinite loop errors, and boundary errors Vulnerabilities (Remote File Checking)

Multiple vulnerabilities have been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

Various types of errors including NULL pointer dereference errors, divide by zero error, infinite loop errors, and boundary errors exist in a multitude of protocol dissectors.

The vulnerabilities have been reported in versions 0.7.7 through 0.10.12.

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

**References:**

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00021.html
http://www.idefense.com/application/poi/display?id=323&type=vulnerabilities

Other references:
http://secunia.com/advisories/16502/
http://secunia.com/advisories/17254/

Product:
http://www.ethereal.com/

**CVE Reference:** CAN-2005-3184, CAN-2005-3241, CAN-2005-3242, CAN-2005-3243, CAN-2005-3244, CAN-2005-3245, CAN-2005-3246, CAN-2005-3247, CAN-2005-3248, CAN-2005-3249

### ❖ 16023 Ethereal "unicode_to_bytes()" boundary error Vulnerabilities (Remote File Checking)

A vulnerability has been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

A boundary error in the "unicode_to_bytes()" function of the SRVLOC (Service Location Protocol) dissector can be exploited to cause a buffer overflow via a specially crafted TCP packet with source and destination port set to 427/tcp.

The vulnerability has been reported in versions 0.7.7 through 0.10.12.

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

**References:**

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00021.html
http://www.idefense.com/application/poi/display?id=323&type=vulnerabilities

Other references:
http://secunia.com/advisories/16502/
http://secunia.com/advisories/17254/

Product:
http://www.ethereal.com/

**CVE Reference:** CAN-2005-3184, CAN-2005-3241, CAN-2005-3242, CAN-2005-3243, CAN-2005-3244, CAN-2005-3245, CAN-2005-3246, CAN-2005-3247, CAN-2005-3248, CAN-2005-3249

### ❖ 16024 Ethereal vulnerable PCRE library Vulnerability (Remote File Checking)

A vulnerability has been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

Ethereal Windows installer ships with a vulnerable version of the PCRE library.

The vulnerability has been reported in versions 0.7.7 through 0.10.12.

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

**References:**

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00021.html
http://www.idefense.com/application/poi/display?id=323&type=vulnerabilities

Other references:
http://secunia.com/advisories/16502/
http://secunia.com/advisories/17254/

Product:
http://www.ethereal.com/

**CVE Reference:** CAN-2005-3184, CAN-2005-3241, CAN-2005-3242, CAN-2005-3243, CAN-2005-3244, CAN-2005-3245, CAN-2005-3246, CAN-2005-3247, CAN-2005-3248,

CAN-2005-3249

# New Vulnerabilities found this Week

- **Skype Multiple Buffer Overflow Vulnerabilities**

  "Denial of Service"

  Some vulnerabilities have been reported in Skype, which can be exploited by malicious people to cause a DoS or to compromise a user's system.

  1) A boundary error exists when handling Skype-specific URI types e.g. "callto://" and "skype://". This can be exploited to cause a buffer overflow and allows arbitrary code execution when the user clicks on a specially-crafted Skype-specific URL.

  2) A boundary error exists in the handling of VCARD imports. This can be exploited to cause a buffer overflow and allows arbitrary code execution when the user imports a specially-crafted VCARD.

  Vulnerability #1 and #2 has been reported in Skype for Windows Release 1.1.*.0 through 1.4.*.83.

  3) An integer overflow error exists when allocating memory in response to certain received Skype client network UDP packet. This can be exploited to cause a heap-based buffer overflow via a specially-crafted UDP packet.

  Successful exploitation crashes the Skype client. It has been reported that the vulnerability is also exploitable via TCP and allows arbitrary code execution via overwritten function pointers on the heap.

  The vulnerability has been reported in the following versions:
  * Skype for Windows Release 1.4.*.83 and prior.
  * Skype for Mac OS X Release 1.3.*.16 and prior.
  * Skype for Linux Release 1.2.*.17 and prior.
  * Skype for Pocket PC Release 1.1.*.6 and prior.

  References:

http://www.skype.com/security/skype-sb-2005-02.html
http://www.skype.com/security/skype-sb-2005-03.html
http://www.pentest.co.uk/documents/ptl-2005-01.html
http://secunia.com/advisories/13191/
http://www.kb.cert.org/vuls/id/668193
http://www.kb.cert.org/vuls/id/905177
http://www.kb.cert.org/vuls/id/930345

- **Snort Back Orifice Pre-Processor Buffer Overflow Vulnerability**

"Boundary error"

Neel Mehta has reported a vulnerability in Snort, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the handling of Back Orifice packets. This can be exploited by sending a maliciously crafted UDP packet to a network or device protected by or running an IDS or IPS system based on Snort.

The vulnerability has been reported in Snort version 2.4.0, 2.4.1, and 2.4.2. Other versions may also be affected.

References:
http://www.snort.org/pub-bin/snortnews.cgi#99
http://xforce.iss.net/xforce/alerts/id/207

- **Sun Solaris HTTP TRACE Response Cross-Site Scripting Issue**

"Cross-site scripting attacks"

Sun has acknowledged a security issue in Solaris, which potentially can be exploited by malicious people to conduct cross-site scripting attacks.

The security issue is caused due to the Solaris Management Console (SMC) webserver responding to HTTP TRACE requests by default. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site when combined with certain browser vulnerabilities. It is reportedly

not possible to disable the TRACE method.

The security issue has been reported in Solaris 8, 9 and 10 on both SPARC and x86 platforms.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102016-1

- **IBM HTTP Server HTTP Request Smuggling Vulnerability**

"Conduct HTTP request smuggling attacks"

IBM has acknowledged a vulnerability in IBM HTTP server, which can be exploited by malicious people to conduct HTTP request smuggling attacks.

Successful exploitation requires that IBM HTTP Server is used as a proxy server.

The vulnerability has been reported in version 1.3.26x and 1.3.28x.

References:
http://www-1.ibm.com/support/docview.wss?uid=swg1PK13959

- **HP Oracle for Openview Multiple Vulnerabilities**

"PL/SQL injection attacks, cross-site scripting attacks"

HP has acknowledged some vulnerabilities in HP OfO (Oracle for Openview), which can be exploited with unknown impact, to conduct PL/SQL injection attacks, cross-site scripting attacks, or potentially to compromise a vulnerable system.

The vulnerability has been reported in versions 8.1.7, 9.1.01, and 9.2 running on HP-UX, Tru64 UNIX, Linux, Solaris, and Windows.

References:
http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBMA01235

❖ **Symantec Discovery Database Accounts Null Password**

"Gain access to, or to manipulate certain information"

A security issue has been reported in Symantec Discovery, which potentially can be exploited by malicious people to gain access to, or to manipulate certain information.

The security issue is caused due to two database accounts, "DiscoveryWeb" and "DiscoveryRO", being created with no passwords during installation. Assigning a password to the "DiscoveryWeb" account will affect the proper functioning of Symantec Discovery.

The security issue has been reported in the following products:
* ON Command Discovery Standard Edition version 4.5.x
* ON Command Discovery Web Edition version 4.5.x
* Symantec Discovery version 6.0

References:
http://securityresponse.symantec.com/avcenter/security/Content/2005.10.24.html

❖ **Fetchmail "fetchmailconf" Password Disclosure Vulnerability**

"Gain knowledge of certain sensitive information"

A vulnerability has been reported in Fetchmail, which can be exploited by malicious, local users to gain knowledge of certain sensitive information.

The vulnerability is caused due to the "fetchmailconf" program writing configuration information to the "run control" file before changing its file permissions to prevent it from being read by other users. This can be exploited by malicious users to gain knowledge of sensitive information such as passwords.

The vulnerability has been reported in the following versions:
* fetchmail version 6.2.5.2
* fetchmail version 6.2.5
* fetchmail version 6.2.0

* fetchmailconf 1.43 (included with fetchmail 6.2.0, 6.2.5 and 6.2.5.2)
* fetchmailconf 1.43.1

Prior versions may also be affected.

References:
http://fetchmail.berlios.de/fetchmail-SA-2005-02.txt

❖ **Linux Kernel IPv6 Denial of Service Vulnerability**

"Denial of Service"

Tetsuo Handa has reported a vulnerability in the Linux Kernel, which potentially can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to an infinite loop error in the "udp_v6_get_port()" function in "net/ipv6/udp.c". This may be exploited to cause a DoS.

The vulnerability affects version 2.6.13.4. Prior versions may also be affected.

References:
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=87bf9c97b4b3af8dec7b2b79cdfe7bfc0a0a03b2

**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