netVigilance

**ScoutNews Team** **November 25, 2005**
**Issue # 47**

Weekly ScoutNews by netVigilance

**Table of Contents**



## This Week in Review

First lawsuits against SONY emerge, IE flaw creates extremely critical vulnerability, Sober is back (again) with numerous email scams and cyber-attacks affecting national security not serious as military secrets get stolen??

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

- **SONY gets sued over DRM fiasco**

  Electronic Frontier Foundation and the State of Texas have filed class action lawsuits against Sony BMG claiming damages caused by the entertainment giants distribution of the XCP Digital Rights Management software included on certain music CDs.

  In the State of Texas suite, Texas attorney general Greg Abbott is seeking $100,000 per violation ( I assume that this means copies sold in the state of Texas – Ed.)

  Designtechnica News

  Full Story :
  http://news.designtechnica.com/article8890.html

## ❖ Un-patched IE flaw now exploitable

Proof of concept code has been published demonstrating an exploit for a six month old vulnerability in Microsoft Internet Explorer. The flaw could potentially allow a malicious remote user to trigger a DoS by way of a JavaScript onload event that calls the window function. According to Johannes Ullrich of the SANS Internet Storm Center (ISC), the flaw allows for arbitrary executables to be executed without user interaction.

IE users are being advised to disable JavaScript on non-trusted sites until a patch is released or use an alternate browser.

InternetNews.com

Full Story:
http://www.internetnews.com/ent-news/article.php/3565846

## ❖ Phony FBI email scam re-surfaces

A Sober WORM variant has emerged this week being spread as a phony unsolicited email from the FBI or CIA. By early Tuesday morning, it was attributed to 35% of all virus infections worldwide as reported by Sophos. If the file that is attached is run, the worm scans the user's hard drive for other email addresses, in its search for other computers to infect.

The FBI takes this matter seriously and is investigating. Users receiving e-mails of this nature are encouraged to report it to the Internet Crime Complaint Center via http://www.ic3.gov.

Related Links:
http://www.securitypark.co.uk/article.asp?articleid=24602&Categoryid=1
http://news.yahoo.com/s/zd/20051122/tc_zd/166036

## ❖ Security expert downplays cyber-threat to national security as Chinese hackers caught stealing military secrets

Purported security expert Bruce Schneider discounts any cyber threats to national

security as 'hyperbole' 'overstated' and 'over-hyped'. Mr. Schneider feels that the criminal threat is 'under-hyped'.

In a related article, a ring of hackers working for the Chinese government was discovered stealing stolen US military secrets, including aviation specifications and flight-planning software from a compromised system at the Redstone Arsenal, home to the Army Aviation and Missile Command.

Related Links:
http://news.zdnet.co.uk/0,39020330,39237490,00.htm
http://news.zdnet.co.uk/0,39020330,39237492,00.htm

# New Vulnerabilities Tested in SecureScout

- **13318 Oracle Database Server - Security component Unspecified error (oct-2005/DB27)**

  An unspecified error in the Security 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

- **13319 Oracle Database Server - Workspace Manager component Unspecified error (oct-2005/DB28)**

  An unspecified error in the Workspace Manager 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

❖ **13320** **Oracle Database Server - Workspace Manager component Unspecified error (oct-2005/DB29)**

An unspecified error in the Workspace Manager 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

❖ **13321** **Oracle Database Server - Oracle HTTP Server component Unspecified error (oct-2005/DB30)**

An unspecified error in the Oracle HTTP Server 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

❖ **13322** **Oracle Database Server - Oracle HTTP Server component Unspecified error (oct-2005/DB31)**

An unspecified error in the Oracle HTTP Server 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

❖ **13323** **Oracle Database Server - Oracle Internet Directory component Unspecified error (oct-2005/DB32)**

An unspecified error in the Oracle Internet Directory 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

❖ **13324** **Oracle Database Server - Oracle Single Sign-On component Unspecified error (oct-2005/DB33)**

An unspecified error in the Oracle Single Sign-On 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

❖ **16037** **Opera Image Control Status Bar Spoofing Weakness (Remote File Checking)**

Claudio "Sverx" has discovered a weakness in Opera, which can be exploited by malicious people to trick users into visiting a malicious website by obfuscating URLs displayed in the status bar.

The problem is that the browser fails to show the correct URL in the status bar if an image control with a "title" attribute has been enclosed in a hyperlink and uses a form to specify the destination URL. This may cause a user to follow a link to a seemingly trusted website when in fact the browser opens a malicious website.

Example:
<form action="[malicious site]">
<a href="[trusted site]"><input type="image" src="[image]" title="[trusted site]"></a>
</form>

The weakness has been confirmed in version 8.5. Other versions may also be affected.

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

**References:**

Original Advisory:
http://secunia.com/advisories/17571/

Product HomePage:
http://www.opera.com/

**CVE Reference:** None

❖ **16038** **Opera Macromedia Flash Player SWF Arbitrary Code Execution (Remote File Checking)**

A vulnerability has been reported in Macromedia Flash Player included in Opera, which can be exploited by malicious people to compromise a user's system and execute arbitrary code.

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

**References:**

Original Advisory:
http://www.kb.cert.org/vuls/id/146284

Other references:
* EEYE:EEYEB-20050627B
*
CONFIRM:http://www.macromedia.com/devnet/security/security_zone/mpsb05-07.html
* BID:15332
* URL:http://www.securityfocus.com/bid/15332
* FRSIRT:ADV-2005-2317
* URL:http://www.frsirt.com/english/advisories/2005/2317

* OSVDB:18825
* URL:http://www.osvdb.org/18825
* SECUNIA:17430
* URL:http://secunia.com/advisories/17430

Product HomePage:
http://www.opera.com/

**CVE Reference:** CAN-2005-2628

❖ **16039** **Internet Explorer Image Control Status Bar Spoofing Weakness (Remote File Checking)**

Claudio "Sverx" has discovered a weakness in Internet Explorer, which can be exploited by malicious people to trick users into visiting a malicious website by obfuscating URLs displayed in the status bar.

The problem is that the browser fails to show the correct URL in the status bar if an image control has been enclosed in a hyperlink and uses a form to specify the destination URL. This may cause a user to follow a link to a seemingly trusted website when in fact the browser opens a malicious website.

Example:
<form action="[malicious site]">
<a href="[trusted site]"><input type="image" src="[image]"></a>
</form>

The weakness has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2.

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

**References:**

Original Advisory:
http://secunia.com/advisories/17565/

Product HomePage:
http://www.microsoft.com/windows/ie/default.mspx

**CVE Reference:** None

# New Vulnerabilities found this Week

**Microsoft Internet Explorer "window()" Arbitrary Code Execution Vulnerability**
"Execute arbitrary code"

Benjamin Tobias Franz has discovered a vulnerability in Internet Explorer, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to certain objects not being initialized correctly when the "window()" function is used in conjunction with the "<body onload>" event. This can be exploited to execute arbitrary code on a vulnerable browser via some specially crafted JavaScript code called directly when a site has been loaded.

Example:
<body onload="window();">

Successful exploitation requires that the user is e.g. tricked into visiting a malicious website.

The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2, and Internet Explorer 6.0 and Microsoft Windows 2000 SP4.

Note: A PoC exploit has been released for this vulnerability.

References:
http://www.computerterrorism.com/research/ie/ct21-11-2005
http://www.microsoft.com/technet/security/advisory/911302.mspx
http://support.microsoft.com/kb/911302
http://www.kb.cert.org/vuls/id/887861

**Opera Command Line URL Shell Command Injection**
"Execute arbitrary shell commands"

Secunia Research has discovered a vulnerability in Opera, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to the shell script used to launch Opera parsing shell commands that are enclosed within backticks in the URL provided via the command line. This can e.g. be exploited to execute arbitrary shell commands by tricking a user into following a malicious link in an external application which uses Opera as the default browser (e.g. the mail client Evolution on Red Hat Enterprise Linux 4).

This vulnerability can only be exploited on Unix / Linux based environments.

The vulnerability has been confirmed in version 8.5 on Red Hat Enterprise Linux 4. Other versions and platforms may also be affected.

References:
http://secunia.com/secunia_research/2005-57/

**Google Mini Search Appliance Multiple Vulnerabilities**
"Cross-site scripting attacks"

H D Moore has reported some vulnerabilities in Google Mini Search Appliance, which can be exploited by malicious people to conduct cross-site scripting attacks and potentially to compromise a vulnerable appliance.

1) Input passed to the "proxystylesheet" parameter isn't properly sanitised before

being returned to the user in an error message. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

2) XSLT style sheets provided by a user using a URL in the "proxystylesheet" parameter isn't properly sanitised before being used. This can be exploited to execute arbitrary Java class methods on a vulnerable appliance via a malicious XSLT style sheet. It is also possible to conduct cross-site scripting attacks by including malicious Javascript in the style sheet.

3) It is possible to enumerate open ports on other systems by providing the full URL containing hostname and port number to a vulnerability appliance and observing the error message.

Note: It is also possible to determine the existence of any file on a vulnerable appliance by providing the relative pathname of the file to the "proxystylesheet" parameter and observing the error message.

References:
http://metasploit.com/research/vulns/google_proxystylesheet/

**Safari Image Control Status Bar Spoofing Weakness**
"Trick users into visiting a malicious website"

A weakness has been reported in Safari, which can be exploited by malicious people to trick users into visiting a malicious website by obfuscating URLs displayed in the status bar.

The problem is that the browser fails to show the correct URL in the status bar if an image control has been enclosed in a hyperlink and uses a form to specify the destination URL. This may cause a user to follow a link to a seemingly trusted website when in fact the browser opens a malicious website.

Example:
<form action="[malicious site]">
<a href="[trusted site]"><input type="image" src="[image]"></a>
</form>

The weakness has been confirmed in version 2.0.2 (416.12). Other versions may also be affected.

References:
http://secunia.com/advisories/17618/

**Sony CD SunnComm MediaMax Uninstallation ActiveX Control Vulnerability**
"Download and execute code"

J. Alex Halderman has reported a vulnerability in SunnComm MediaMax's uninstallation ActiveX control, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a design error in the AxWebRemoveCtrl ActiveX control that is installed via Internet Explorer when the user un-installs the

MediaMax software by visiting the vendor's website. This may be exploited to download and execute code from an arbitrary URL.

Successful exploitation requires that the user is e.g. tricked into visiting a malicious website.

References:
http://www.freedom-to-tinker.com/?p=931

**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