netVigilance

ScoutNews Team **March 26, 2005**
Issue # 12

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Be careful if you are a Yahoo messenger user, a new, simpler data encryption tool emerges and will the US Government address weak information security before it's too late?

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

- **Yahoo Messenger users target of Phishing Scam**

Yahoo announced on Thursday that a Phishing scam is being launched against users of the popular free messaging service. Users receive a message that appears to come from someone on the users friends list asking them to click on a url redirecting them to a phony website.

The website appears to be a legitimate Yahoo site and prompts for username / password. The hackers steal login credentials and gain access to personal information and user's friends lists.

ZDNet Australia

Related Links :
http://www.techzonez.com/comments.php?shownews=12626
http://news.com.com/Phishers+target+Yahoo+Messenger/2100-7349_3-5634007.html

- **UK Company introduces easy-to-use data encryption tool.**

Data Encryption Systems (DES) of Somerset, UK has introduced a new version of its DESKey, DESLock products that enable data encryption of files and data; transparent to the user.

The public-private key system comes in two versions; personal and business. The personal version uses a single key file stored on your hard drive; provided for free from the DES website. The Business version; uses USB token devices to store and exchange encryption keys.

DESlock+ protects your data with transparent file, folder and email encryption. Designed for fast, on-the-fly encryption, it can be used to encrypt any data including personal files, corporate information, confidential records and email attachments.

Up to 64 different encryption keys, stored in a USB security token, allow confidential information to be shared with a large number of exclusive users or groups

The software allows you to encrypt files or folders on the local hard drive, and a plug-in also allows users to send encrypted emails and attachments from Microsoft Outlook or Lotus Notes.

IT Week

Related Links:
http://www.des.co.uk/
http://www.vnunet.com/news/1162161

- **Is there a pending Dam-Burst in our nation's cyber security?**

Charles Cooper of CNET warns of a lack of attention to US cyber security. A report delivered to President Bush entitled "Cyber Security: A Crisis of Prioritization," warns of the current vulnerable state of national information security and recommends fundamental changes to how systems get deployed.

The present administration does not seem to set this as a high priority. Read more here:
http://sympatico-msn-ca.com.com/A+cyber+con+game/2010-1071_3-5635833.html?part=sympatico-msn-ca&tag=feed_2517&subj=ns

CNET News.com

New Vulnerabilities Tested in SecureScout

- **15299 Mozilla Thunderbird GIF Image Processing Buffer Overflow Vulnerability (Remote File Checking)**

  Mark Dowd has reported a vulnerability in Thunderbird, which can be exploited by malicious people to compromise a user's system.

  The vulnerability is caused due to a boundary error in the GIF image processing of Netscape extension 2 blocks and can be exploited to cause a heap-based buffer overflow via a specially crafted image.

  Successful exploitation may allow execution of arbitrary code.

  The vulnerability has been reported in versions prior to 1.0.2.

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

  References:

  Original Advisory:
  http://www.mozilla.org/security/announce/mfsa2005-30.html
  http://xforce.iss.net/xforce/alerts/id/191

  Product HomePage:
  http://www.mozilla.org/products/thunderbird/

  Other references:
  http://secunia.com/advisories/14685/

CVE Reference: CAN-2005-0399

❖ **15496 Mozilla Security Bypass Vulnerability (Remote File Checking)**

An error in the restriction of privileged XUL files can e.g. be exploited to open a local privileged XUL file by tricking a user into dragging a faked scrollbar.

The vulnerability itself does not pose any direct security risk as no XUL files in the product use external parameters in an insecure way nor do any destructive actions when being opened.

Successful exploitation may allow execution of arbitrary code.

The vulnerabilities have been reported in versions prior to 1.7.6.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-32.html

Product HomePage:
http://www.mozilla.org/products/thunderbird/

Other references:
http://secunia.com/advisories/14684/

CVE Reference: CAN-2005-0401

❖ **15497 Mozilla GIF Image Processing Buffer Overflow Vulnerability (Remote File Checking)**

A boundary error in the GIF image processing of Netscape extension 2 blocks can be exploited to cause a heap-based buffer overflow via a specially crafted image.

Successful exploitation may allow execution of arbitrary code.

The vulnerabilities have been reported in versions prior to 1.7.6.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-30.html
http://xforce.iss.net/xforce/alerts/id/191

Product HomePage:
http://www.mozilla.org/products/thunderbird/

Other references:
http://secunia.com/advisories/14684/

CVE Reference: CAN-2005-0399

❖ **15498 Mozilla Firefox local privileged XUL file Vulnerability (Remote File Checking)**

An error in the restriction of privileged XUL files can e.g. be exploited to open a local privileged XUL file by tricking a user into dragging a faked scrollbar.

The vulnerability itself does not pose any direct security risk as no XUL files in the product use external parameters in an insecure way nor do any destructive actions when being opened.

Successful exploitation may allow execution of arbitrary code.

The vulnerabilities have been reported in versions prior to 1.0.2.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-32.html

Product HomePage:
http://www.mozilla.org/products/thunderbird/

Other references:
http://secunia.com/advisories/14654/

CVE Reference: CAN-2005-0401

❖ **15499 Mozilla Firefox sidebar panel Vulnerability (Remote File Checking)**

A web site added as a sidebar panel can load privileged content, which can be exploited to execute arbitrary programs by injecting JavaScript into a privileged URL.

Successful exploitation may allow execution of arbitrary code.

The vulnerabilities have been reported in versions prior to 1.0.2.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-31.html

Product HomePage:
http://www.mozilla.org/products/thunderbird/

Other references:
http://secunia.com/advisories/14654/

CVE Reference: CAN-2005-0402

❖ **15578 Mozilla Firefox GIF image processing Vulnerability (Remote File Checking)**

A boundary error in the GIF image processing of Netscape extension 2 blocks can be exploited to cause a heap-based buffer overflow via a specially crafted image.

Successful exploitation may allow execution of arbitrary code.

The vulnerabilities have been reported in versions prior to 1.0.2.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-30.html
http://xforce.iss.net/xforce/alerts/id/191

Product HomePage:
http://www.mozilla.org/products/thunderbird/

Other references:
http://secunia.com/advisories/14654/

CVE Reference: CAN-2005-0399

❖ **15579 Mozilla Thunderbird Drag and Drop Vulnerability (Remote File Checking)**

A vulnerability has been reported in Thunderbird, which can be exploited by malicious people to plant malware on a user's system.

The vulnerabilities have been reported in versions prior to 1.0.2.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-25.html

Product HomePage:
http://www.mozilla.org/products/thunderbird/

Other references:
http://secunia.com/advisories/14671/

CVE Reference: CAN-2005-0230

❖ **15580 Mozilla Secure Site Icon Vulnerability (Remote File Checking)**

A bug was found in the way Mozilla displays the secure site icon. A malicious web page can display the secure site icon by loading a binary file from a secured site.

This affetcs Mozilla prior to version 1.7.6.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-14.html

Product HomePage:
http://www.mozilla.org/products/mozilla1.x/

Other references:
https://bugzilla.mozilla.org/show_bug.cgi?id=258048
https://bugzilla.mozilla.org/show_bug.cgi?id=268483
https://bugzilla.mozilla.org/show_bug.cgi?id=277564
https://bugzilla.mozilla.org/show_bug.cgi?id=276720

CVE Reference: CAN-2005-0143

❖ **15581 Mozilla Firefox Secure Site Icon Vulnerability (Remote File Checking)**

A bug was found in the way Firefox displays the secure site icon. A malicious web page can display the secure site icon by loading a binary file from a secured site.

This affetcs Firefox prior to version 1.0.1.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-14.html

Product HomePage:
http://www.mozilla.org/products/firefox/

Other references:
https://bugzilla.mozilla.org/show_bug.cgi?id=258048
https://bugzilla.mozilla.org/show_bug.cgi?id=268483
https://bugzilla.mozilla.org/show_bug.cgi?id=277564
https://bugzilla.mozilla.org/show_bug.cgi?id=276720

CVE Reference: CAN-2005-0143

- **15582 Mozilla tag followed by a null character Vulnerability (Remote File Checking)**

Mozilla allows remote attackers to cause a denial of service (application crash from null dereference or infinite loop) via a web page that contains a (1) TEXTAREA, (2) INPUT, (3) FRAMESET or (4) IMG tag followed by a null character and some trailing characters, as demonstrated by mangleme.

This affetcs Mozilla prior to version 1.7.6

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

References:

Original Advisory:
http://www.securityfocus.com/bid/11439

Product HomePage:
http://www.mozilla.org/products/mozilla1.x/

Other references:
http://marc.theaimsgroup.com/?l=bugtraq&m=109811406620511&w=2
http://securitytracker.com/alerts/2004/Oct/1011810.html
http://xforce.iss.net/xforce/xfdb/17805

CVE Reference: CAN-2004-1613

New Vulnerabilities found this Week

❖ **Mozilla Thunderbird GIF Image Processing Buffer Overflow Vulnerability**
"heap-based buffer overflow"

Mark Dowd has reported a vulnerability in Thunderbird, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the GIF image processing of Netscape extension 2 blocks and can be exploited to cause a heap-based buffer overflow via a specially crafted image.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been reported in versions prior to 1.0.2.

References:
http://www.mozilla.org/security/announce/mfsa2005-30.html
http://xforce.iss.net/xforce/alerts/id/191

❖ **Mozilla Security Bypass and Buffer Overflow Vulnerabilities**
"open a local privileged XUL file, heap-based buffer overflow"

Two vulnerabilities have been reported in Mozilla, which can be exploited by malicious people to bypass certain security restrictions and compromise a user's system.

1) An error in the restriction of privileged XUL files can e.g. be exploited to open a local privileged XUL file by tricking a user into dragging a faked scrollbar.

The vulnerability itself does not pose any direct security risk as no XUL files in the product use external parameters in an insecure way nor do any destructive actions when being opened.

2) A boundary error in the GIF image processing of Netscape extension 2 blocks can be exploited to cause a heap-based buffer overflow via a specially crafted image.

Successful exploitation may allow execution of arbitrary code.

The vulnerabilities have been reported in versions prior to 1.7.6.

References:
http://www.mozilla.org/security/announce/mfsa2005-32.html
http://www.mozilla.org/security/announce/mfsa2005-30.html
http://xforce.iss.net/xforce/alerts/id/191

❖ **Mozilla Firefox Three Vulnerabilities**
"bypass certain security restrictions"

Three vulnerabilities have been reported in Firefox, which can be exploited by malicious people to bypass certain security restrictions and compromise a user's system.

1) An error in the restriction of privileged XUL files can e.g. be exploited to open a local privileged XUL file by tricking a user into dragging a faked scrollbar.

The vulnerability itself does not pose any direct security risk as no XUL files in the product use external parameters in an insecure way nor do any destructive actions when being opened.

2) A web site added as a sidebar panel can load privileged content, which can be exploited to execute arbitrary programs by injecting JavaScript into a privileged URL.

3) A boundary error in the GIF image processing of Netscape extension 2 blocks can be exploited to cause a heap-based buffer overflow via a specially crafted image.

Successful exploitation may allow execution of arbitrary code.

The vulnerabilities have been reported in versions prior to 1.0.2.

References:
http://www.mozilla.org/security/announce/mfsa2005-32.html
http://www.mozilla.org/security/announce/mfsa2005-31.html
http://www.mozilla.org/security/announce/mfsa2005-30.html
http://xforce.iss.net/xforce/alerts/id/191

❖ **Sun Java System Application Server Cross-Site Scripting**
"cross-site scripting attacks"

Eric Hobbs has reported a vulnerability in Sun Java System Application Server, which can be exploited by malicious people to conduct cross-site scripting attacks.

The vulnerability is caused due to an unspecified input validation error and can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site.

The following versions are affected:
* Sun Java System Application Server Standard Edition 7 Update Release 5 and prior
* Sun Java System Application Server Platform Edition 7 Update Release 5 and prior
* Sun Java System Application Server 7 2004Q2 Standard Edition Update Release 1 and prior

* Sun Java System Application Server 7 2004Q2 Enterprise Edition Update Release 1 and prior

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57742-1

❖ **SurgeMail Three Vulnerabilities**
"cross-site scripting attacks, script insertion attacks, bypass certain security restrictions"

Tan Chew Keong has reported three vulnerabilities in SurgeMail, which can be exploited by malicious people to conduct cross-site scripting attacks and by malicious users to conduct script insertion attacks, bypass certain security restrictions, and gain knowledge of various information.

1) An input validation error in the webmail functionality when handling attachment uploads can be exploited via directory traversal attacks to disclose the contents of some directories, retrieve certain files, and upload files to arbitrary locations.

2) An input validation error in the auto-reply configuration functionality can be exploited by a user to inject arbitrary HTML and script code in the auto-reply message, which may be executed in an administrative user's browser session in context of a vulnerable site when viewing a user's auto-reply settings.

3) Input passed to the "page" parameter of "webmail.exe" is not properly sanitised before being returned to users. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site.

References:
http://www.security.org.sg/vuln/surgemail22g3.html

❖ **Sun Solaris newgrp Privilege Escalation Vulnerability**
"gain escalated privileges"

A vulnerability has been reported in Sun Solaris, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to an unspecified boundary error in the newgrp utility and can be exploited to cause a buffer overflow.

Successful exploitation allows execution of arbitrary code with root privileges.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57710-1

❖ **Java Web Start JNLP File Command Line Argument Injection Vulnerability**
"pass arbitrary command line arguments to the virtual machine"

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.

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

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