netVigilance

ScoutNews Team **September 23, 2005**
Issue # 38

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Security Software demo brought down during onstage demo, more companies coming out about cyber crime, from the double-O files: keyboard keystroke listening, airport departure lounge computers a collection of secrets and Bagle is loose again in a big way.

Be careful out there and 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

- **Ouch! - That's gonna' leave a mark**

While onstage at Demofall 2005 demonstrating how their software can avert a simulated attack on a network, Redwood City, Calif.-based Determina, was hacked in a real-life DoS attack.

I love how this stuff just writes itself – Ed.

cnet

Full Story:
http://beta.news.com.com/2061-10789_3-5876638.html

❖ Increase in reported cyber-crime losses

Reported cyber crime attacks jumped to 862 incidents from 704 for the same period a year ago. This may be due to several factors; an increased awareness on the part of corporations, legal requirements such as California SB1386 and the New York Information Security Breach and Notification Act or less fear of public disclosure.

redherring

Full Story:
http://www.redherring.com/Article.aspx?a=13555&hed=Security+Threats+Rise+22%25+&sector=Industries&subsector=SecurityAndDefense

❖ Listening device detects keystokes by sound alone

In a breakthrough that would make James Bond himself envious, experts at UC Berkeley have developed a listening device that can discern the unique sounds of different keyboards strokes. Although not perfect, this does raise concern for another potential hacking methodology.

CBC News

Full Story :
http://www.cbc.ca/story/science/national/2005/09/21/keyboard_secrets_20050921.html

❖ PCs in airport executive lounges hold many secrets

PCs located in airport departure lounges are found to be filled with sensitive information, virus' and users email messages.

Security on these machines is non-existent and users tend to be high-level executives handling confidential data.

The Register

Full Story:
http://www.securityfocus.com/news/11324

❖ Bagle variant running wild

New bagle variants hit the web Monday and Tuesday of this week causing a bit of a scramble for AV signature makers. The latest variations attempt to disable anti-virus software, turn target PCs into zombies and download more malware.

Source

Related Links:
http://www.securityfocus.com/news/11325
http://news.zdnet.com/2100-1009_22-5766772.html

New Vulnerabilities Tested in SecureScout

- **15233 PHP "php_handle_iff()" function Vulnerability**

Multiple vulnerabilities have been reported in PHP, where some have an unknown impact and others can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

Errors within the "php_handle_iff()" function called by the "getimagesize()" PHP function can be exploited to cause infinite loops and consume all available CPU resources via a specially crafted image.

This has been reported in versions 4.2.2, 4.3.9, 4.3.10, and 5.0.3. Other versions may also be affected.

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

References:

Advisory:
http://www.php.net/release_4_3_11.php
http://www.idefense.com/application/poi/display?id=222&type=vulnerabilities

Other references:
http://secunia.com/advisories/14792/

Product Page:
http://www.php.net/

CVE Reference: CAN-2005-0524

- **15234 PHP "php_handle_jpeg()" function Vulnerability**

Multiple vulnerabilities have been reported in PHP, where some have an unknown impact and others can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

Errors within the "php_handle_jpeg()" function called by the "getimagesize()" PHP function can be exploited to cause infinite loops and consume all available CPU resources via a specially crafted image.

This has been reported in versions 4.2.2, 4.3.9, 4.3.10, and 5.0.3. Other versions may also be affected.

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

References:

Advisory:
http://www.php.net/release_4_3_11.php
http://www.idefense.com/application/poi/display?id=222&type=vulnerabilities

Other references:
http://secunia.com/advisories/14792/

Product Page:
http://www.php.net/

CVE Reference: CAN-2005-0525

❖ 15235 PHP "exif_process_IFD_TAG()" function Vulnerability

Multiple vulnerabilities have been reported in PHP, where some have an unknown impact and others can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

An integer overflow in the "exif_process_IFD_TAG()" function in "exif.c" in the exif extension may be exploited to execute arbitrary code via an application processing EXIF tags of uploaded images.

Versions 4.3.11 or 5.0.4. fix the issue.

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

References:

Advisory:
http://www.php.net/release_4_3_11.php

Other references:
http://secunia.com/advisories/14792/

Product Page:
http://www.php.net/

CVE Reference: CAN-2005-1042

❖ 15236 PHP processing of exif data in "exif.c" Vulnerability

Multiple vulnerabilities have been reported in PHP, where some have an unknown impact and others can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

An error in the processing of exif data in "exif.c" may be exploited to cause an infinite stack recursion via an application processing EXIF headers of uploaded images.

Versions 4.3.11 or 5.0.4. fix the issue.

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

References:

Advisory:
http://www.php.net/release_4_3_11.php

Other references:
http://secunia.com/advisories/14792/

Product Page:
http://www.php.net/

CVE Reference: CAN-2005-1043

❖ 15237 PHP fbsql extensions Vulnerability

Multiple vulnerabilities have been reported in PHP, where some have an unknown impact and others can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

Multiple unspecified security issues exist in the fbsql extensions.

Versions 4.3.11 or 5.0.4. fix the issue.

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

References:

Advisory:
http://www.php.net/release_4_3_11.php

Other references:
http://secunia.com/advisories/14792/

Product Page:
http://www.php.net/

CVE Reference: None

❖ 15238 PHP "unserialize()" function Vulnerability

Multiple vulnerabilities have been reported in PHP, where some have an unknown impact and others can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

Multiple unspecified security issues exist in the "unserialize()" function.

Versions 4.3.11 or 5.0.4. fix the issue.

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

References:

Advisory:
http://www.php.net/release_4_3_11.php

Other references:
http://secunia.com/advisories/14792/

Product Page:
http://www.php.net/

CVE Reference: None

❖ 15239 PHP "swf_definepoly()" function Vulnerability

Multiple vulnerabilities have been reported in PHP, where some have an unknown impact and others can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

Multiple unspecified security issues exist in the "swf_definepoly()" function.

Versions 4.3.11 or 5.0.4. fix the issue.

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

References:

Advisory:
http://www.php.net/release_4_3_11.php

Other references:
http://secunia.com/advisories/14792/

Product Page:
http://www.php.net/

CVE Reference: None

❖ 15686 Opera Mail Client Attachment Script Insertion (Remote File Checking)

Secunia Research has discovered a vulnerability in the Opera Mail client, which can be exploited by a malicious person to conduct script insertion attacks.

Attached files are opened without any warnings directly from the user's cache directory. This can be exploited to execute arbitrary JavaScript in context of "file://".

The vulnerability has been confirmed in Opera version 8.02, prior versions may also be vulnerable.

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

References:

Original Advisory:
http://secunia.com/secunia_research/2005-42/

Other references:
http://secunia.com/advisories/16645/

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

CVE Reference: None

❖ 15687 Opera Mail Client Attachment Spoofing (Remote File Checking)

Secunia Research has discovered a vulnerability in the Opera Mail client, which can be exploited by a malicious person to spoof the name of attached files.

Normally, filename extensions are determined by the "Content-Type" in Opera Mail. However, by appending an additional '.' to the end of a filename, an HTML file could be spoofed to be e.g. "image.jpg.".

The vulnerability have been confirmed in Opera version 8.02, prior versions may also be vulnerable.

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

References:

Original Advisory:
http://secunia.com/secunia_research/2005-42/

Other references:
http://secunia.com/advisories/16645/

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

CVE Reference: None

❖ 15688 Opera Image Dragging Vulnerability (Remote File Checking)

Secunia Research has discovered a vulnerability in Opera, which can be exploited by malicious people to conduct cross-site scripting attacks and retrieve a user's files.

The vulnerability is caused due to Opera allowing a user to drag e.g. an image, which is actually a "javascript:" URI, resulting in cross-site scripting if dropped over another site. This may also be used to populate a file upload form, resulting in uploading of arbitrary files to a malicious web site.

Successful exploitation requires that the user is tricked into dragging and dropping e.g. an image or a link.

The vulnerability has been confirmed in version 8.01. Prior versions may also be affected.

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

References:

Original Advisory:
http://secunia.com/advisories/15756/

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

CVE Reference: CAN-2005-2406

New Vulnerabilities found this Week

- **Firefox Command Line URL Shell Command Injection**

"Execute arbitrary shell commands"

Peter Zelezny has discovered a vulnerability in Firefox, 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 Firefox 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 Firefox 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 1.0.6 on Fedora Core 4 and Red Hat Enterprise Linux 4. Other versions and platforms may also be affected.

References:
https://bugzilla.mozilla.org/show_bug.cgi?id=307185

- **Thunderbird Command Line URL Shell Command Injection**

"Execute arbitrary shell commands"

A vulnerability has been discovered in Thunderbird, 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 Thunderbird is 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 with the "mailto:" URI handler in an external application which uses Thunderbird as the default mail reader (e.g. Firefox on Fedora Core 4).

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

The vulnerability has been confirmed in version 1.0.6 on Fedora Core 4. Other versions and platforms may also be affected.

References:
https://bugzilla.mozilla.org/show_bug.cgi?id=307185

❖ Linux Kernel "fget()" Potential Denial of Service Vulnerability

“Denial of Service”

Vasiliy Averin 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 the missing use of "sockfd_put()" in "routing_ioctl()" on 64-bit platforms. This may be exploited to overrun a reference counter via a large number of fget() requests. Subsequent call to fput() will cause resources to be incorrectly freed, which can potentially crash the kernel. Similar vulnerability exists in "tiocgdev()" on x86-64 platforms.

The vulnerability only affects 64-bit platforms.

References:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13.2

❖ Mozilla Command Line URL Shell Command Injection

“Execute arbitrary shell commands”

A vulnerability has been discovered in Mozilla Suite, which can be exploited by malicious people to compromise a user's system.

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

The vulnerability has been confirmed in version 1.7.11. Other versions may also affected.

References:
http://secunia.com/advisories/16869/

❖ Opera Mail Client Attachment Spoofing and Script Insertion

“Conduct script insertion attacks and to spoof the name of attached files”

Secunia Research has discovered two vulnerabilities in the Opera Mail client, which can be exploited by a malicious person to conduct script insertion attacks and to spoof the name of attached files.

1. Attached files are opened without any warnings directly from the user's cache directory. This can be exploited to execute arbitrary JavaScript in context of "file://".

2. Normally, filename extensions are determined by the "Content-Type" in Opera Mail. However, by appending an additional '.' to the end of a filename, an HTML file could be spoofed to be e.g. "image.jpg.".

The two vulnerabilities combined may be exploited to conduct script insertion attacks if the user chooses to view an attachment named e.g. "image.jpg." e.g. resulting in disclosure of local files.

The vulnerabilities have been confirmed in Opera version 8.02, prior versions may also be

vulnerable.

References:
http://secunia.com/secunia_research/2005-42/

❖ Safari "data:" URI Handler Denial of Service Weakness

"Denial of Service"

Jonathan Rockway has discovered a weakness in Safari, which can be exploited by malicious people to cause a DoS (Denial of Service).

The weakness is caused due to an error in the processing of URLs in the "data:" URI handler. This can be exploited to crash a vulnerable browser via e.g. an image tag referencing a specially crafted "data:" URL.

Example:
data://<h1>crash</h1>

The weakness has been confirmed in version 2.0 (412.2). Other versions may also be affected.

References:
http://secunia.com/advisories/16875/

❖ Sun Solaris "tl" Driver Denial of Service Vulnerability

"Denial of Service"

A vulnerability has been reported in Solaris, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error in the "tl" driver. This can be exploited by non-privileged users to cause a system panic.

The vulnerability has been reported in Solaris 10 on SPARC and x86 architectures.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101899-1&searchclause

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