netVigilance

ScoutNews Team

March 3, 2006
2006 Issue # 9

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review
Top Security News Stories this Week
New Test Cases Tested in SecureScout
New Vulnerabilities this Week

This Week in Review

Large corporations found not funding IT security adequately, AOL is first to get aggressive toward phishers, become a hacker for under $1000 and from the "getta' load of this guy" files – university professor promotes cyber crime.

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

- **Survey finds IT Security under funded**

Computer Economics recently published their *IT Security Study* that shows mid-sized businesses are doing the best job of network security.

56% of the participants admit that network security is under-funded and that budgetary constraints are causing compromises in security. A whopping 86% responded that they feel cyber threats will continue to get worse.

CIO Update

Full Story :
http://www.cioupdate.com/research/article.php/3587176

❖ AOL breaks ground in pursuing Phishers

In filing 3 separate lawsuits against three phishing gangs; AOL emerges as the first major ISP to take direct action against suspected scammer.

The action was sparked by reports from AOL customers that the phishing emails were targeting them.

RedHerring

Full Story :
http://www.redherring.com/Article.aspx?a=15895&hed=AOL+Reels+in+Phishers&sector=Industries&subsector=SecurityAndDefense

❖ Malware for Sale

A organization calling itself PandaLabs has published an application known as Trj/Briz.A; a piece of malware that specializes in stealing bank details and data from web forms.

So for $990 you too can become an infamous cyber thief or ace your computer security course from "Professor Packetslinger" (below).

SC Magazine

Full Story :
http://www.scmagazine.com/uk/news/article/543448/crimeware-code-sells-trojans-hackers/

❖ Professor promotes criminal hacking for grade

SANS gives us a report this week about a university professor that assigned his students homework requiring them to perform attack reconnaissance on an Internet server. (!?!)

The name of the professor in question; as well as the institution where he teaches, is being kept secret. It may be hard for students to opt-out since it is reported that the assignment accounts for 15% of the grade.

This stuff is worth the read if only for the entertainment value. (Do I get work-study credit for doing Hard Time? – *Ed.*)

SecurityFocus, SANS

Related Links :
http://www.securityfocus.com/brief/151

New Vulnerabilities Tested in SecureScout

- **16139 Linux Kernel Socket Data Buffering Denial of Service Vulnerability**

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

The vulnerability is caused due to missing memory availability checking when buffering data for transfer over a pair of sockets. This can be exploited by malicious users to cause a DoS (memory exhaustion) by creating a large number of connected file descriptors or socketpairs that use the largest possible kernel buffer for the data transfer.

The vulnerability has been reported in version 2.4.22 and 2.6.12. Other versions may also be affected.

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

References:

Original advisory:
http://www.idefense.com/intelligence/vulnerabilities/display.php?id=362

Other references:
http://secunia.com/advisories/18205/
* BID:16041
* URL:http://www.securityfocus.com/bid/16041
* FRSIRT:ADV-2005-3076
* URL:http://www.frsirt.com/english/advisories/2005/3076
* SECTRACK:1015402
* URL:http://securitytracker.com/id?1015402

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-3660

- **16140 Linux Kernel missing validation of the "nlmsg_len" value in "netlink_rcv_skb()" Vulnerability**

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

Missing validation of the "nlmsg_len" value in "netlink_rcv_skb()" can cause an infinite loop. This can be exploited by local users to cause a DoS by setting the value to 0.

Version 2.6.15.1 of the Linux Kernel fixes the issue.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.15.1

Other references:
http://secunia.com/advisories/18482/
* TRUSTIX:2006-0004
* URL:http://www.trustix.org/errata/2006/0004

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2006-0035

❖ 16141 Linux Kernel error in the PPTP NAT helper Vulnerability

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

An error in the PPTP NAT helper in the handling of inbound PPTP_IN_CALL_REQUEST packets can cause an error in offset calculation. This can be exploited to cause random memory corruption and can crash the kernel.

Version 2.6.15.1 of the Linux Kernel fixes the issue.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Medium** Risk: **Dos, Crash**

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.15.1

Other references:
http://secunia.com/advisories/18482/
* TRUSTIX:2006-0004
* URL:http://www.trustix.org/errata/2006/0004

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2006-0036

❖ 16142 Linux Kernel error exists in the PPTP NAT helper when calculating offsets Vulnerability

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

An error exists in the PPTP NAT helper when calculating offsets based on the difference between two pointers to the header. This can result in the wrong offset being used, which can potentially crash the kernel via illegal memory access.

Version 2.6.15.1 of the Linux Kernel fixes the issue.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Medium** Risk: **Dos, Crash**

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.15.1

Other references:
http://secunia.com/advisories/18482/
TRUSTIX:2006-0004
URL:http://www.trustix.org/errata/2006/0004

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2006-0037

❖ 16143 Linux Kernel Information Disclosure Vulnerability

A vulnerability has been reported in the Linux Kernel, which can be exploited by malicious, local users to disclose potentially sensitive information.

The "dm-crypt" driver fails to clear memory before freeing it. This can be exploited by local users to obtain sensitive information (e.g. cryptographic keys).

The vulnerability has been reported in version 2.6.15.1. Other versions may also be affected.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.16-rc1

Other references:
http://secunia.com/advisories/18487/
* MLIST:[linux-kernel] 20060104 [Patch 2.6] dm-crypt: zero key before freeing it
* URL:http://marc.theaimsgroup.com/?l=linux-kernel&m=113640535312572&w=2
* MLIST:[linux-kernel] 20060104 [Patch 2.6] dm-crypt: Zero key material before free to avoid information leak
* URL:http://marc.theaimsgroup.com/?l=linux-kernel&m=113641114812886&w=2
* MANDRIVA:MDKSA-2006:040
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:040
* TRUSTIX:2006-0004
* URL:http://www.trustix.org/errata/2006/0004
* UBUNTU:USN-244-1
* URL:http://www.ubuntulinux.org/support/documentation/usn/usn-244-1

* BID:16301
* URL:http://www.securityfocus.com/bid/16301
* FRSIRT:ADV-2006-0235
* URL:http://www.frsirt.com/english/advisories/2006/0235

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2006-009

❖ 16144 Linux Kernel error in the "mq_open" system to cause a kernel panic Vulnerability

A vulnerability has been reported in the Linux Kernel, which can be exploited by malicious, local users to DoS cause a Denial of Service.

An error in the "mq_open" system call can cause the "mqueue_mnt->mnt_count" counter to be decremented twice when the "dentry_open" function call fails. This can potentially be exploited by malicious users to cause a kernel panic.

The vulnerability has been reported in version 2.6.15.1. Other versions may also be affected.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Medium** Risk: **Dos, Crash**

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.16-rc1

Other references:
http://secunia.com/advisories/18487/
* CONFIRM:http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=7c7dce9209161eb260cdf9e9172f72c3a02379e6
* CONFIRM:http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=169130
* MANDRIVA:MDKSA-2006:040
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:040
* REDHAT:RHSA-2006:0101
* URL:http://rhn.redhat.com/errata/RHSA-2006-0101.html
* SUSE:SuSE-SA:2006:006
* URL:http://www.novell.com/linux/security/advisories/2006_06_kernel.html
* UBUNTU:USN-244-1
* URL:http://www.ubuntulinux.org/support/documentation/usn/usn-244-1
* BID:16283
* URL:http://www.securityfocus.com/bid/16283

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3356

❖ 16145 Linux Kernel "search_binary_handler()" Denial of Service

Vulnerability

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

The vulnerability is caused due to missing validation of the return code of a function call in the "search_binary_handler()" function of exec.c. This can be exploited by local users to cause a kernel panic via certain commands.

The vulnerability has been reported in version 2.4.21. Other versions may also be affected.

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

References:

Original advisory:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=161925

Other references:
http://secunia.com/advisories/18523/
* CONFIRM:https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=161925
* REDHAT:RHSA-2006:0140
* URL:http://www.redhat.com/support/errata/RHSA-2006-0140.html
* REDHAT:RHSA-2006:0190
* URL:http://www.redhat.com/support/errata/RHSA-2006-0190.html
* BID:16320
* URL:http://www.securityfocus.com/bid/16320

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-2708

❖ 16146 Linux Kernel ICMP Error Handling Denial of Service Vulnerability

A vulnerability has been reported in the Linux Kernel, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due an error in the handling of an error condition when constructing an ICMP response in the "ip_options_echo()" function of icmp.c. This can be exploited to cause a DoS via specially crafted ICMP packets containing record-route or timestamp IP options.

The vulnerability affects versions 2.6.12 through 2.6.15.2.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.15.3

Other references:
http://secunia.com/advisories/18766/
* MLIST:[linux-kernel] 20060207 Linux 2.6.15.3
* URL:http://marc.theaimsgroup.com/?l=linux-kernel&m=113927617401569&w=2
* MLIST:[linux-kernel] 20060207 Re: Linux 2.6.15.3
* URL:http://marc.theaimsgroup.com/?l=linux-kernel&m=113927648820694&w=2
* MLIST:[dailydave] 20060207 Fun with Linux (2.6.12 -> 2.6.15.2)
* URL:http://lists.immunitysec.com/pipermail/dailydave/2006-February/002909.html
* CONFIRM:http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.15.3
* MANDRIVA:MDKSA-2006:040
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:040
* SUSE:SuSE-SA:2006:006
* URL:http://www.novell.com/linux/security/advisories/2006_06_kernel.html
* UBUNTU:USN-250-1
* URL:http://www.ubuntu.com/usn/usn-250-1
* BID:16532
* URL:http://www.securityfocus.com/bid/16532
* FRSIRT:ADV-2006-0464
* URL:http://www.frsirt.com/english/advisories/2006/0464

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2006-0454

❖ 16147 Linux Kernel error in the "nfs_get_user_pages()" function to cause a local DoS Vulnerability

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

An error in the "nfs_get_user_pages()" function due to insufficient checks on the return value returned by the "get_user_pages()" function can be exploited to cause a local DoS by performing an O_DIRECT write to an NFS file where the user buffer starts with a valid mapped page, but also contains an unmapped page.

The vulnerability affects versions 2.6 through 2.6.15.5 not included.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.15.5

Other references:
http://secunia.com/advisories/19083/

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2006-0554, CVE-2006-0555, CVE-2006-0741

❖ **16148 Linux Kernel missing checks for bad elf entry addresses to cause DoS Vulnerability**

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

Missing checks for bad elf entry addresses can be exploited to cause an endless recursive fault on Intel systems, which results in a local DoS.

The vulnerability affects versions 2.6 through 2.6.15.5 not included.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.15.5

Other references:
http://secunia.com/advisories/19083/

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2006-0554, CVE-2006-0555, CVE-2006-0741

New Vulnerabilities found this Week

Mac OS X Security Update Fixes Multiple Vulnerabilities
"Denial of Service; arbitrary code execution"

Apple has issued a security update for Mac OS X, which fixes multiple vulnerabilities.

1) Various security issues exist in the PHP Apache module and scripting environment.

2) An error in automount makes it possible for malicious file servers to cause a vulnerable system to mount file systems with reserved names, which can cause a DoS (Denial of Service) or potentially allow arbitrary code execution.

3) An input validation error in the BOM framework when unpacking certain archives can be exploited to cause files to be unpacked to arbitrary locations via directory traversal attacks.

4) The "passwd" program creates temporary files insecurely, which can be exploited via symlink attacks to create or overwrite arbitrary files with "root" privileges.

5) User directories are insecurely mounted when a FileVault image is created, which may allow unauthorised access to files.

6) An error in IPSec when handling certain error conditions can be exploited to cause a DoS against VPN connections.

7) An error in the LibSystem component can be exploited by malicious people to cause a heap-based buffer overflow via applications when requesting large amounts of memory. This can potentially be exploited to execute arbitrary code in the context of a vulnerable application.

8) The "Download Validation" in the Mail component fails to warn users about unsafe file types when an e-mail attachment is double-clicked.

9) In certain cases a Perl program may fail to drop privileges.

10) A boundary error in rsync can be exploited by authenticated users to cause a heap-based buffer overflow when it's allowed to transfer extended attributes. This can be exploited to crash the rsync service or execute arbitrary code.

11) A boundary error in WebKit's handling of certain HTML can be exploited to cause a heap-based buffer overflow. This can be exploited via a malicious web site to execute arbitrary code on a user's system.

12) A boundary error in Safari when parsing JavaScript can be exploited to cause a stack-based buffer overflow and allows execution of arbitrary code when a malicious web page including specially crafted JavaScript is viewed.

13) An error in Safari's security model when handling HTTP redirection can be exploited to execute JavaScript in the local domain via a specially crafted web site.

14) An error in Safari / LaunchServices may cause a malicious application to appear as a safe file type. This may cause a malicious file to be executed automatically when the "Open safe files after downloading" option is enabled.

15) An input validation error in the Syndication (Safari RSS) component can be exploited to conduct cross-site scripting attacks when subscribing to malicious RSS content.

References:
http://docs.info.apple.com/article.html?artnum=303382

Linux Kernel Local Denial of Service Vulnerabilities
"Denial of Service"

Some vulnerabilities have been reported in the Linux kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

1) An error in the "nfs_get_user_pages()" function due to insufficient checks on the return value returned by the "get_user_pages()" function can be exploited to cause a local DoS by performing an O_DIRECT write to an NFS file where the user buffer starts with a valid mapped page, but also contains an unmapped page.

2) Missing checks for bad elf entry addresses can be exploited to cause an endless recursive fault on Intel systems, which results in a local DoS.

An error in the XFS "ftruncate()" function, which may expose stale data off disk to users, has also been reported.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.15.5

MySQL Query Logging Bypass Security Issue
"Bypass certain security restrictions"

1dt.w0lf has discovered a security issue in MySQL, which can be exploited by malicious users to bypass certain security restrictions.

The security issue is caused due to an error within the handling of query logging. This can be exploited to cause part of the query to be incorrectly logged if the query contains the NULL character.

Example:
mysql_query("/*".chr(0)."*/ SELECT * FROM table");

The security issue has been confirmed in version 5.0.18. Other versions may also be affected.

References:
http://rst.void.ru/papers/advisory39.txt

phpRPC Library Arbitrary Code Execution Vulnerability
"Execute arbitrary PHP code"

James Bercegay has reported a vulnerability in phpRPC, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an error within the "decode()" function in rpc_decoder.php when decoding received XML data. This can be exploited to execute arbitrary PHP code via a specially-crafted XML request.

The vulnerability has been reported in version 0.7 and prior. Other versions may also be affected.

References:
http://www.gulftech.org/?node=research&article_id=00105-02262006

FreeBSD "nfsd" NFS Mount Request Denial of Service
"Denial of Service"

Evgeny Legerov has reported a vulnerability in FreeBSD, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to a NULL pointer dereference error within the handling of NFS mount requests. This can be exploited to cause a kernel panic via a request with a zero-length payload sent to the "nfsd" daemon on port 2049/tcp.

References:
ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:10.nfs.asc

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