netVigilance

ScoutNews Team **December 16, 2005**
Issue # 50

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

The worms continue to eat at AIM, Feds [still] failing on computer security and is Wardriving a crime?

Stay Vigilant!

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

- **AOL Worm exhibits haunting new attack**

A new AOL IM worm called IM.myspace04.AIM was spotted this week; sending users a message encouraging them to click on an enclosed link. The disturbing thing about this new attack is the method by which it circumvents AOL's prescribed method of avoiding phishing attacks that is; asking the sender what it is and why they're sending it to you.

In the case of IM.myspace04.AIM, the Worm is smart enough to answer back to such questions appearing to be the trusted person from your 'buddy list'. AOL experts recommend keeping your anti-virus software updated and regularly scanning for spyware.

CRN

Full Story :

http://abcnews.go.com/Technology/Business/story?id=1402737

❖ US Government blasted for poor cybersecurity

Cyber Security Industry Alliance (CSIA) panned the Federal Government for it's poor performance on cyber-security for the past year. Citing the fact that The Department of Homeland Security (DHS) has failed to hire an assistant secretary, a 'crisis' state of research and development and lack of leadership; the CSIA report gave six Ds, one F and only one of the remaining five, scored above C. Reading the report, one gets the impression that the Feds are running one huge honeypot.

TECHWORLD

Related Links:
http://www.techworld.com/security/news/index.cfm?NewsID=4996&inkc=0

❖ Not all hacks are preceded by port scans

A study done University of Maryland's A. James Clark School of Engineering shows that port scans precede attacks only about 5 percent of the time.

Source

Related Links:
http://www.computerworld.com.au/index.php/id%3b1592416211%3bfp%3b2%3bfpid%3b1

❖ Are you a 'Wardriver?'

Roger Dooley blogs about the legality of Wardriving; the practice of looking for an open wireless access point by driving around in a car with a wireless laptop computer.

The net-net thus far depends on your intention and impact on the unprotected Wireless Access Points (WAP).

(My thanks to Roger for coming clean and admitting his own Wardriving; makes me feel more comfortable about admitting to it myself – *Ed.*)

Source

Related Links:

http://www.rogerd.net/articles/legality-of-wardriving

New Vulnerabilities Tested in SecureScout

❖ 16042 Linux Kernel Ptrace Privilege Escalation Vulnerability

A vulnerability has been identified in version 2.2.x and 2.4.x of the Linux kernel.

The vulnerability is caused by an error in ptrace and can be exploited by malicious, local users to escalate their privileges to "root" on a vulnerable system.

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/315635

Other references:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0127
* VULNWATCH:20030317 Fwd: Ptrace hole / Linux 2.2.25
* URL:http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0134.html
* REDHAT:RHSA-2003:098
* URL:http://rhn.redhat.com/errata/RHSA-2003-098.html
* REDHAT:RHSA-2003:088
* URL:http://rhn.redhat.com/errata/RHSA-2003-088.html
* SUSE:SuSE-SA:2003:021
* ENGARDE:ESA-20030318-009
* DEBIAN:DSA-270
* URL:http://www.debian.org/security/2003/dsa-270
* DEBIAN:DSA-276
* URL:http://www.debian.org/security/2003/dsa-276
* DEBIAN:DSA-311
* URL:http://www.debian.org/security/2003/dsa-311
* DEBIAN:DSA-312
* URL:http://www.debian.org/security/2003/dsa-312
* DEBIAN:DSA-332
* URL:http://www.debian.org/security/2003/dsa-332
* DEBIAN:DSA-336
* URL:http://www.debian.org/security/2003/dsa-336
* DEBIAN:DSA-423
* URL:http://www.debian.org/security/2004/dsa-423
* DEBIAN:DSA-495
* URL:http://www.debian.org/security/2004/dsa-495
* MANDRAKE:MDKSA-2003:038
* URL:http://www.mandrakesoft.com/security/advisories?name=MDKSA-2003:038
* MANDRAKE:MDKSA-2003:039
* URL:http://www.mandrakesoft.com/security/advisories?name=MDKSA-2003:039
* CALDERA:CSSA-2003-020.0
* URL:ftp://ftp.caldera.com/pub/security/OpenLinux/CSSA-2003-020.0.txt
* ENGARDE:ESA-20030515-017
* URL:http://marc.theaimsgroup.com/?l=bugtraq&m=105301461726555&w=2
* REDHAT:RHSA-2003:145

* URL:http://www.redhat.com/support/errata/RHSA-2003-145.html
* GENTOO:GLSA-200303-17
* URL:http://security.gentoo.org/glsa/glsa-200303-17.xml
* CERT-VN:VU#628849
* URL:http://www.kb.cert.org/vuls/id/628849
* OVAL:OVAL254
* URL:http://oval.mitre.org/oval/definitions/data/oval254.html

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2003-0127

❖ 16043 Cumulative Security Update for Internet Explorer (MS05-054/905915) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer displays file download dialog boxes and accepts user input during interaction with a Web page. This interaction could be in the form of certain keystrokes that a user makes when visiting a Web page. A custom dialog box may also be positioned in front of a file download dialog box to make this more convincing. A user may also be persuaded to double-click an element of a Web page.

An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction is required to exploit this vulnerability.

An information disclosure vulnerability exists in the way Internet Explorer behaves in certain situations where an HTTPS proxy server requires clients to use Basic authentication. This vulnerability could allow an attacker to read Web addresses in clear text sent from Internet Explorer to a proxy server despite the connection being an HTTPS connection.

A remote code execution vulnerability exists in the way Internet Explorer instantiates COM objects that are not intended to be instantiated in Internet Explorer. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A remote code execution vulnerability exists in the way Internet Explorer handles mismatched Document Object Model objects. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-054.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2829
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2830
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2831
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1790

CVE Reference: CAN-2005-2829, CAN-2005-2830, CAN-2005-2831, CAN-2005-1790

❖ 16044 Vulnerability in Windows Kernel Could Allow Elevation of Privilege (MS05-055/908523) (Remote File Checking)

A privilege elevation vulnerability exists in the way that asynchronous procedure calls are processed within the kernel. This vulnerability could allow a logged on user to take complete control of the system.

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

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-055.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2827

CVE Reference: CAN-2005-2827

❖ 16045 Linux Kernel dangling ptrace references Vulnerability

An error in the auto-reap of child processes that have ptrace attached can lead to dangling ptrace references. This may be exploited by local users to cause a kernel crash.

The vulnerability has been reported in the 2.6 kernel branch and has been fixed in version 2.6.15-rc3.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.15-rc3
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=7ed0175a462c4c30f6df6fac1cccac058f997739
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=f3a9388e4ebea57583272007311fffa26ebbb305
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=479ef592f3664dd629417098c8599261c0f689ab
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.15-rc2
http://kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=dc15ae14e97ee9d5ed740cbb0b94996076d8b37e

Other references:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174078
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174337

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3784, CAN-2005-3807, CVE-2005-3857

❖ 16046 Linux Kernel "printk()" in the "time_out_leases()" function consuming a large amount of kernel log space Vulnerability

The use of "printk()" in the "time_out_leases()" function in "/fs/locks.c" can consume a large amount of kernel log space. This can be exploited by local users to cause a DoS by generating a large number of broken leases.

The vulnerability has been reported in the 2.6 kernel branch and has been fixed in version 2.6.15-rc3.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.15-rc3
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=7ed0175a462c4c30f6df6fac1cccac058f997739
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=f3a9388e4ebea57583272007311fffa26ebbb305
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=479ef592f3664dd629417098c8599261c0f689ab
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.15-rc2
http://kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=dc15ae14e97ee9d5ed740cbb0b94996076d8b37e

Other references:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174078
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174337

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3784, CAN-2005-3807, CVE-2005-3857

❖ 16047 Linux Kernel memory leak error in the VFS file lease handling code Vulnerability

A memory leak error exists in the VFS file lease handling code in "/fs/locks.c". This may be exploited by local users to cause a DoS (memory exhaustion) by performing certain Samba requests that causes an "fasync" entry to be re-allocated by the "fcntl_setlease()" function after the "fasync" queue has already been cleaned by the "locks_delete_lock()" function.

The vulnerability has been reported in the 2.6 kernel branch and has been fixed in version 2.6.15-rc3.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.15-rc3
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=7ed0175a462c4c30f6df6fac1cccac058f997739
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=f3a9388e4ebea57583272007311fffa26ebbb305
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=479ef592f3664dd629417098c8599261c0f689ab
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.15-rc2
http://kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=dc15ae14e97ee9d5ed740cbb0b94996076d8b37e

Other references:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174078
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174337

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3784, CAN-2005-3807, CVE-2005-3857

❖ 16048 Linux Kernel integer overflow error in the "invalidate_inode_pages2_range()" function Vulnerability

An integer overflow error exists in the "invalidate_inode_pages2_range()" function of "/mm/truncate.c". This can be exploited by local users to cause a DoS.

The vulnerability has been reported in the 2.6 kernel branch and has been fixed in version 2.6.15-rc3.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.15-rc3
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=7ed0175a462c4c30f6df6fac1cccac058f997739
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=f3a9388e4ebea57583272007311fffa26ebbb305
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=479ef592f3664dd629417098c8599261c0f689ab
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.15-rc2
http://kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=dc15ae14e97ee9d5ed740cbb0b94996076d8b37e

Other references:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174078

https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174337

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3784, CAN-2005-3807, CVE-2005-3857

❖ 16049 Linux Kernel sysctl Interface Unregistration Denial of Service Vulnerability

A vulnerability has been reported 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 error in "sysctl.c" when handling the un-registration of interfaces in "/proc/sys/net/ipv4/conf/". This can potentially be exploited by malicious users to cause a DoS.

The vulnerability has been reported in the 2.6 kernel branch and has been fixed in version 2.6.14.1.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.14.1
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.14.y.git;a=commit;h=e4e0411221c7d4f2bd82fa5e21745f927a1bff28

Other references:
http://secunia.com/advisories/17504/

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-2709

❖ 17733 Bugzilla summary of a "secure" bug Vulnerability

Bugzilla is a free, open source bug tracking and reporting application. It allows users to submit bugs, offers a forum for discussing bugs, keeps track of the bug status, and can restrict who has access to bug information.

It is possible to view the summary of a "secure" bug if an email address is supplied, which previously has been used to vote on the bug.

The vulnerability has been reported in various versions prior to 2.17.5 and 2.16.4.

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

References:

Original advisory:
http://bugzilla.mozilla.org/show_bug.cgi?id=209376

Other references:
http://secunia.com/advisories/10149/

Product HomePage:
http://www.bugzilla.org/

CVE Reference: None

❖ 17734 Bugzilla view component descriptions for a product Vulnerability

Bugzilla is a free, open source bug tracking and reporting application. It allows users to submit bugs, offers a forum for discussing bugs, keeps track of the bug status, and can restrict who has access to bug information.

An unspecified vulnerability may allow users to view component descriptions for a product, which the user doesn't have access to.

The vulnerability has been reported in various versions prior to 2.17.5 and 2.16.4.

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

References:

Original advisory:
http://bugzilla.mozilla.org/show_bug.cgi?id=209742

Other references:
http://secunia.com/advisories/10149/

Product HomePage:
http://www.bugzilla.org/

CVE Reference: None

New Vulnerabilities found this Week

Microsoft Internet Explorer Multiple Vulnerabilities
“View potentially sensitive information, to trick users into downloading and executing arbitrary programs”

Five vulnerabilities have been reported in Microsoft Internet Explorer, which can be exploited by malicious people to view potentially sensitive information, to trick users into downloading and executing arbitrary programs, and to compromise a user's system.

1) A design error in the processing of keyboard shortcuts for certain security dialogs can e.g. be exploited to delay the "File Download" dialog box and trick users into executing a malicious ".bat" file after pressing the "r" key.

2) A design error in the processing of mouse clicks in new browser windows and the predictability of the position of the "File Download" dialog box can be exploited to trick the user into clicking on the "Run" button of the dialog box. This is exploited by first causing a "File Download" dialog box to be displayed underneath a new browser window, and then tricking the user into double-clicking within a specific area in the new window. This will result in an unintended click of the "Run" button in the hidden "File Download" dialog box.

3) An error exists in Internet Explorer when used with a HTTPS proxy server that requires clients to use Basic Authentication. This may cause web addresses that are sent from Internet Explorer to be disclosed to a third-party even when HTTPS connection is used.

4) An error exists when certain COM objects that are not intended to be used with Internet Explorer are instantiated in Internet Explorer. This can be exploited to execute arbitrary code via a malicious webpage that instantiates a vulnerable COM object.

5) An error exists in the initialisation of certain objects when the "window()" function is used in conjunction with the "<body onload>" event. This can be exploited to execute arbitrary code via a malicious webpage.

The vulnerabilities #1, #2, and #5 have been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2. Other versions may also be affected.

References:
http://secunia.com/secunia_research/2005-7/advisory/
http://secunia.com/secunia_research/2005-21/advisory/
http://www.microsoft.com/technet/security/Bulletin/MS05-054.mspx

Microsoft Windows Kernel APC Queue List Handling Privilege Escalation
“Gain escalated privileges**”**

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

The vulnerability is caused due to an error in the thread termination routine in the Kernel when freeing entries in the APC (Asynchronous Procedure Call) queue list. This can be exploited to alter arbitrary kernel memory, potentially allowing the execution flow to be altered via a malicious program

Successful exploitation allows a malicious user to gain escalated privileges but requires a valid logon to the affected system.

References:
http://www.microsoft.com/technet/security/Bulletin/MS05-055.mspx
http://www.eeye.com/html/research/advisories/AD20051213.html

SSH Tectia Server Host-Based Authentication Security Issue

“Gain escalated privileges”

A security issue has been reported in SSH Tectia Server, which can be exploited by malicious users to bypass certain security restrictions and potentially to gain escalated privileges.

The security issue is caused due to an error in the handling of host-based authentication. This may cause a user to be logged on with wrong credentials to a server running SSH Tectia Server.

Successful exploitation requires that host-based authentication is enabled and the user must logon from an authorised host.

The security issue has been reported in version 5.0.0 (A, F, and T) on Windows, Linux and Unix platforms.

References:
http://secunia.com/advisories/18001/

MySQL Auction "keyword" Cross-Site Scripting Vulnerability
“Conduct cross-site scripting attacks”

r0t has reported a vulnerability in MySQL Auction, which can be exploited by malicious people to conduct cross-site scripting attacks.

Input passed to the "keyword" parameter when performing a search isn't properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerability have been reported in version 3.0 and prior. Other versions may also be affected.

References:
http://pridels.blogspot.com/2005/12/mysql-auction-xss-vuln.html

Apache mod_imap "Referer" Cross-Site Scripting Vulnerability
“Conduct cross-site scripting attacks”

A vulnerability has been reported in Apache httpd, which can be exploited by malicious people to conduct cross-site scripting attacks.

Input passed to the image map "Referer" directive in "mod_imap" isn't properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerability has been reported in versions 1.3.0 through 1.3.34, and versions 2.0.35 through 2.0.55.

References:
http://www.apacheweek.com/features/security-13
http://www.apacheweek.com/features/security-20

Mac OS X Perl "$<" Privilege Dropping Security Issue

"Bypass certain security restrictions"

Jason Self has reported a security issue in Mac OS X, which can be exploited by malicious people to bypass certain security restrictions.

The security issue is caused due to the Perl binary included with Mac OS X not correctly dropping privileges when a Perl application uses the "$< = numeric_id;" statement to set its uid. The issue may be caused due to wrong compilation options being selected when compiling the Perl binary.

The security issue has been reported in the Perl binary included with Mac OS X Server 10.3.9. Prior versions may also be affected.

Note: The actual impact depends on how a Perl application is written to use the affected Perl functionality.

References:
http://secunia.com/advisories/17922/

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