netVigilance

ScoutNews Team **January 13, 2006** **2006 Issue # 2**

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

WMF still holey, gadgets becoming popular targets for hackers, security firms enter rootkit business and part of Atlantis lost again.

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

❖ More Microsoft wmf bugs found

Less than a week after the release of a patch for the MS zero-day wmf vulnerability, 2 more bugs are found. Not as serious as the infamous December 27th exploit; these can lead to DoS attacks using flaws in the Microsoft Windows Meta File (WMF) format for image files.

Red Herring

Full Story :
http://www.redherring.com/Article.aspx?a=15239&hed=More+Security+Bugs+Hit+Windows&sector=Industries&subsector=SecurityAndDefense

❖ Cyber crooks targeting Xbox, iPod and Linux says Gov

The annual Cyber Crime Conference focused on these extremely popular but often unsupervised operating systems. Hackers tend to gravitate to connected devices that are not in the forefront of network security such as a PC running windows.

One unique and possibly troubling feature of these devices is that they are connected and disconnected to networks, removing with them the source of an infection or data theft.

Eweek.com

Full Story :

http://www.eweek.com/article2/0,1895,1910371,00.asp

❖ Symantec, Kspersky accused of Spyware tactics

The terrible immoralities are the cunning ones hiding behind masks of morality, such as exploiting people while pretending to help them.
-*Vernon Howard*

Even though they both contend that their products install secret software; is not a rootkit since it "was not designed with malicious intent". Symantec has issued a patch (yes patch) to remove the cloaking software and Kaspersky was considering similar action.

Unlike the SONY XCP product which hides executable code, the Symantec and Kaspersky products hide only data that they have collected.

IDG - NetworkWorld

Full Story :

http://www.networkworld.com/news/2006/011206-symantec-kaspersky.html?fsrc=netflash-rss

❖ Atlantis resort drops identities of 55,000 guests

Kerzner International Ltd., which operates the Atlantis resort on Paradise Island in the Bahamas, reported the theft last week in a U.S. regulatory filing that they detected the theft of addresses, credit card numbers, SSNs, bank account numbers and drivers license numbers of approximately 55,000 guests.

The resort said it was notifying affected customers in writing so that they can "take steps to protect themselves from possible identity fraud." (Because obviously, they can't –Ed.)

Security.itworld.com

Related Links :
http://security.itworld.com/5010/060111bahamas/page_1.html

New Vulnerabilities Tested in SecureScout

❖ 16080 Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution (MS06-001/912919) (Remote File Checking)

A remote code execution vulnerability exists in the Graphics Rendering Engine because of the way that it handles Windows Metafile (WMF) images. An attacker could exploit the vulnerability by constructing a specially crafted WMF image that could potentially allow remote code execution if a user visited a malicious Web site or opened a specially crafted attachment in e-mail. 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, Gain Root**

References:

http://www.microsoft.com/technet/security/Bulletin/MS06-001.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4560

CVE Reference: CVE-2005-4560

❖ 16081 Linux Kernel error in "mm/mempolicy.c" to cause kernel panic 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), gain knowledge of potentially sensitive information.

An error in "mm/mempolicy.c" when handling the policy system call may cause the referencing of undefined nodes. This can potentially be exploited by local users to cause kernel panic via a "set_mempolicy()" call with a 0 bitmask.

The vulnerability has been fixed in version 2.6.15.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.15
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=8f493d797bc1fe470377adc9d8775845427e240e
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=ea86575eaf99a9262a969309d934318028dbfacb
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-

2.6.git;a=commit;h=8febdd85adaa41fa1fc1cb31286210fc2cd3ed0c
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=5c15c0b4fa850543b8ccfcf93686d24456cc384d
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=8b90db0df7187a01fb7177f1f812123138f562cf

Other references:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=175683
http://secunia.com/advisories/18216/

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3358, CVE-2005-4605

❖ 16082 Linux Kernel error in "net/ipv4/fib_frontend.c" to cause illegal memory references 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), gain knowledge of potentially sensitive information.

An error in "net/ipv4/fib_frontend.c" when validating the header and payload of fib_lookup netlink messages may result in illegal memory references via malformed netlink messages.

The vulnerability has been fixed in version 2.6.15.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.15
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=8f493d797bc1fe470377adc9d8775845427e240e
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=ea86575eaf99a9262a969309d934318028dbfacb
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=8febdd85adaa41fa1fc1cb31286210fc2cd3ed0c
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=5c15c0b4fa850543b8ccfcf93686d24456cc384d
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=8b90db0df7187a01fb7177f1f812123138f562cf

Other references:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=175683
http://secunia.com/advisories/18216/

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3358, CVE-2005-460

❖ 16083 Linux Kernel error in "kernel/sysctl.c" to cause user supplied buffer overflow 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), gain knowledge of potentially sensitive information.

An off-by-one error in "kernel/sysctl.c" may cause the user supplied buffer to be overflowed with a single NULL byte when the output string is too large to fit in the buffer.

The vulnerability has been fixed in version 2.6.15.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.15
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=8f493d797bc1fe470377adc9d8775845427e240e
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=ea86575eaf99a9262a969309d934318028dbfacb
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=8febdd85adaa41fa1fc1cb31286210fc2cd3ed0c
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=5c15c0b4fa850543b8ccfcf93686d24456cc384d
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=8b90db0df7187a01fb7177f1f812123138f562cf

Other references:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=175683
http://secunia.com/advisories/18216/

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3358, CVE-2005-4605

❖ 16084 Linux Kernel boundary error in the CA-driver for TwinHan DST Frontend/Card to cause buffer overflow 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), gain knowledge of potentially sensitive information.

A boundary error in the CA-driver for TwinHan DST Frontend/Card, "drivers/media/dvb/bt8xx/dst_ca.c", may cause a buffer overflow when more than 8 bytes are read into an 8 byte long array.

The vulnerability has been fixed in version 2.6.15.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.15
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=8f493d797bc1fe470377adc9d8775845427e240e
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=ea86575eaf99a9262a969309d934318028dbfacb
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=8febdd85adaa41fa1fc1cb31286210fc2cd3ed0c
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=5c15c0b4fa850543b8ccfcf93686d24456cc384d
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=8b90db0df7187a01fb7177f1f812123138f562cf

Other references:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=175683
http://secunia.com/advisories/18216/

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3358, CVE-2005-460

❖ 16085 Linux Kernel unspecified error in the procfs code may allow local users to read kernel memory 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), gain knowledge of potentially sensitive information.

An unspecified error in the procfs code may allow local users to read kernel memory, which may contain sensitive information.

The vulnerability has been fixed in version 2.6.15.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.15
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=8f493d797bc1fe470377adc9d8775845427e240e
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=ea86575eaf99a9262a969309d934318028dbfacb
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=8febdd85adaa41fa1fc1cb31286210fc2cd3ed0c
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=5c15c0b4fa850543b8ccfcf93686d24456cc384d

http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=8b90db0df7187a01fb7177f1f812123138f562cf

Other references:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=175683
http://secunia.com/advisories/18216/

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3358, CVE-2005-4605

❖ 16086 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.

The vulnerability has been fixed in version 2.6.15 and 2.4.32.

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

References:

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

Other references:
http://secunia.com/advisories/18205/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-3660

❖ 16087 Linux Kernel xfrm Array Indexing Overflow Vulnerability

Balazs Scheidler 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 a boundary error in the XFRM code and can be exploited to cause an array indexing overflow.

The vulnerability has been fixed in version 2.6.12.4.

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

References:

Original advisory:
http://www.mail-archive.com/netdev@vger.kernel.org/msg00520.html
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.4

Other references:
http://secunia.com/advisories/16298/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2456

❖ 16121 Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution (MS06-002/908519) (Remote File Checking)

A remote code execution vulnerability exists in Windows because of the way that it handles malformed embedded Web fonts. An attacker could exploit the vulnerability by constructing a malicious embedded Web font that could potentially allow remote code execution if a user visited a malicious Web site or viewed a specially crafted e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system

Test Case Impact: **Gather Info.** Vulnerability Impact: **High** Risk: **Malicious Code**

References:

http://www.microsoft.com/technet/security/Bulletin/MS06-002.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0010

CVE Reference: CVE-2006-0010

❖ 16122 Vulnerability in TNEF Decoding in Microsoft Outlook and Microsoft Exchange Could Allow Remote Code Execution (MS06-003/902412) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Outlook and Microsoft Exchange Server because of the way that it decodes the Transport Neutral Encapsulation Format (TNEF) MIME attachment.

An attacker could exploit the vulnerability by constructing a specially crafted TNEF message that could potentially allow remote code execution when a user opens or previews a malicious e-mail message or when the Microsoft Exchange Server Information Store processes the specially crafted message.

An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Test Case Impact: **Gather Info.** Vulnerability Impact: **High** Risk: **Malicious Code**

References:

http://www.microsoft.com/technet/security/Bulletin/MS06-003.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0010

CVE Reference: xxxxxxxxxxxxxxxxxxxxx

New Vulnerabilities found this Week

Microsoft Outlook / Exchange TNEF Decoding Arbitrary Code Execution Vulnerability
“Execute arbitrary code”

A vulnerability has been reported in Microsoft Outlook / Exchange, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to boundary error when decoding the Transport Neutral Encapsulation Format (TNEF) MIME attachment. This can be exploited to execute arbitrary code when the user opens or previews a specially crafted TNEF email message or when the Microsoft Exchange Server Information Store processes the message.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-003.mspx
http://www.kb.cert.org/vuls/id/252146

Microsoft Windows Embedded Web Fonts Arbitrary Code Execution Vulnerability
“Execution arbitrary code”

A vulnerability has been reported in Microsoft Windows, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in T2EMBED.DLL when handling malformed embedded Web fonts. This can be exploited to cause a heap-based buffer overflow and allows execution arbitrary code when a user visits a malicious website or views an e-mail message that contains a specially-crafted embedded Web font.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-002.mspx
http://www.eeye.com/html/research/advisories/AD20060110.html
http://www.piotrbania.com/all/adv/MS06-002-adv.txt
http://www.kb.cert.org/vuls/id/915930

Sun Solaris Unspecified Privilege Escalation and Denial of Service
“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) and gain escalated privileges.

The vulnerability is caused due to an unspecified error and can be exploited by unprivileged users to gain root privileges or panic the operating system.

The vulnerability has been reported in the following versions and affects only the x86 platform.
* Solaris 9 (with patch 112234-11 or 112234-12 or 117172-16 or later)
* Solaris 10

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102066-1

Sun Solaris "/proc" Filesystem Searching 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 when the find(1) command is used to perform a search on the "/proc" filesystem. This can be exploited by malicious unprivileged users to cause a DoS.

The vulnerability has been reported in Solaris 10 on both the SPARC and x86 platforms.

PostgreSQL Multiple Connections Denial of Service Vulnerability

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

The vulnerability is caused due to an error in the handling of multiple concurrent connections. This can be exploited to shutdown the postmaster process.

Successful exploitation causes a situation where new connections can't be established until the service is manually restarted.

The vulnerability has been reported in versions 8.0.0 through 8.0.5 and 8.1.0 through 8.1.1. This only affects the Microsoft Windows platform.

References:
http://archives.postgresql.org/pgsql-announce/2006-01/msg00001.php

Apache auth_ldap Module "auth_ldap_log_reason()" Format String Vulnerability
“Execute arbitrary code”

Seregorn has reported a vulnerability in the auth_ldap module for Apache, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a format string error in the "auth_ldap_log_reason()" function. This can be exploited to execute arbitrary code by e.g. supplying a specially crafted username in the authentication process.

The vulnerability has been reported in versions 1.2.x through 1.6.0. Prior versions may also be affected.

References:
http://www.digitalarmaments.com/2006090173928420.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