netVigilance

ScoutNews Team **December 22, 2005**
Issue # 51

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

Observations in network security, Guidance Software gets breached and Symantec AV hole discovered.

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

❖ Important lessons in network security

Matthew Friedman gives us lessons learned from some of the more serious computer security breaches of the recent past.

The net-net; examine and test all processes especially avenues where Social Engineering attacks can be used to exploit your security measures.

Networking Pipeline

Full Story :

http://www.smallbizpipeline.com/175006398?cid=rssfeed_pl_sbp

❖ eCase software maker gets hacked

Guidance Software; a maker of forensic software, fell victim to a hacker attack where the perpetrators made off with roughly 3,800 customer credit cards records.The theft resulted in about $20,000 in unauthorized transactions.

It seems a bit careless to me to hack in to a security company that counts the U.S. Secret Service, the FBI and New York City police – *Ed.*
Source

Full Story:
http://www.washingtonpost.com/wp-dyn/content/article/2005/12/19/AR2005121900928.html?nav=rss_technology

- **Symantec AV flaw discovered**

A former employee of the security software giant discovered a vulnerability in Symantec's Avit-Virus products that could enable a virus or worm hidden inside a specially crafted RAR file to allow attackers to take complete control over infected computers.

Full Story:

http://blogs.washingtonpost.com/securityfix/2005/12/symantec_antivi.html

New Vulnerabilities Tested in SecureScout

- **16050 Linux Kernel missing parameter validation in the "map_to_seg7()" function Vulnerability**

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

A boundary error due to missing parameter validation in the "map_to_seg7()" function in "drivers/usb/input/map_to_7segment.h" of the Yealink driver may cause out-of-bound memory references.

The vulnerability has been reported in the 2.6 kernel branch and has been fixed in version 2.6.14-git4.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/snapshots/patch-2.6.14-git4.log
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-

2.6.git;a=commit;h=af64a5ebb817532965d18b792d6d74afecfb0bcf
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=5c50d1885981537ff3b8df6433951de6c9cb72cb
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.14
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=25f407f0b668f5e4ebd5d13e1fb4306ba6427ead
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.14.y.git;a=commit;h=788e05a67c343fa22f2ae1d3ca264e7f15c25eaf

Other references:
http://secunia.com/advisories/17384/

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3527, CVE-2005-3805, CAN-2005-3847

❖ 16051 Linux Kernel handling of SMBus Block Write transactions Vulnerability

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

A boundary error in "/drivers/i2c/i2c-core.c" when handling SMBus Block Write transactions may cause a buffer overflow.

The vulnerability has been reported in the 2.6 kernel branch and has been fixed in version 2.6.14-git4

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

References:

References: Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/snapshots/patch-2.6.14-git4.log
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=af64a5ebb817532965d18b792d6d74afecfb0bcf
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=5c50d1885981537ff3b8df6433951de6c9cb72cb
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.14
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=25f407f0b668f5e4ebd5d13e1fb4306ba6427ead
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.14.y.git;a=commit;h=788e05a67c343fa22f2ae1d3ca264e7f15c25eaf

Other references:
http://secunia.com/advisories/17384/

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3527, CVE-2005-3805, CAN-2005-3847

❖ 16052 Linux Kernel handling of locking in the POSIX timer cleanup code Vulnerability

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

An error exists in the handling of locking in the POSIX timer cleanup code when running on SMP systems. This may 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 2.6.14-git4.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/snapshots/patch-2.6.14-git4.log
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=af64a5ebb817532965d18b792d6d74afecfb0bcf
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=5c50d1885981537ff3b8df6433951de6c9cb72cb
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.14
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=25f407f0b668f5e4ebd5d13e1fb4306ba6427ead
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.14.y.git;a=commit;h=788e05a67c343fa22f2ae1d3ca264e7f15c25eaf

Other references:
http://secunia.com/advisories/17384/

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3527, CVE-2005-3805, CAN-2005-3847

❖ 16053 Linux Kernel race condition in the "do_coredump()" function Vulnerability

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

A race condition in the "do_coredump()" function in "/kernel/signal.c" can be exploited by malicious users to cause a DoS by triggering a core dump in one thread while another thread has a pending SIGSTOP.

The vulnerability has been reported in the 2.6 kernel branch and has been fixed in version 2.6.14-git4.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/snapshots/patch-2.6.14-git4.log
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=af64a5ebb817532965d18b792d6d74afecfb0bcf
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=5c50d1885981537ff3b8df6433951de6c9cb72cb
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.14
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=25f407f0b668f5e4ebd5d13e1fb4306ba6427ead
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.14.y.git;a=commit;h=788e05a67c343fa22f2ae1d3ca264e7f15c25eaf

Other references:
http://secunia.com/advisories/17384/

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3527, CVE-2005-3805, CAN-2005-3847

❖ 16054 Linux Kernel IPv6 Denial of Service Vulnerability

Tetsuo Handa 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 an infinite loop error in the "udp_v6_get_port()" function in "net/ipv6/udp.c". This may be exploited to cause a DoS.

The vulnerability affects version 2.2.26 and prior, version 2.4.32-rc1 and prior, and version 2.6.13.4 and prior.

The vulnerability has been fixed in version 2.4.32-rc2 or 2.6.14-rc5.

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

References:

Original advisory:
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=87bf9c97b4b3af8dec7b2b79cdfe7bfc0a0a03b2
http://www.kernel.org/git/?p=linux/kernel/git/marcelo/linux-2.4.git;a=commit;h=2d5a5e7918796127b64e996f6a9f00d5e95161ed
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=170772

Other references:
http://secunia.com/advisories/17261/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2973

❖ 16055 Linux Kernel Console Keyboard Mapping Shell Command

Injection Vulnerability

Rudolf Polzer has reported a vulnerability in the Linux Kernel, which potentially can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to the way console keyboard mapping is handled. The keyboard map installed by a local user using "loadkeys" is applied to all virtual consoles and is not being reset after the user logs out.

Successful exploitation allows malicious console users to inject arbitrary shell commands into certain key mappings, which are executed when the next logon console user uses the re-mapped key.

The vulnerability has been fixed in version 2.4.32-rc2 and in version 2.6.14-git12.

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

References:

Original advisory:
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=334113
http://kernel.org/pub/linux/kernel/v2.6/snapshots/patch-2.6.14-git12.log
http://kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=0b360adbdb54d5b98b78d57ba0916bc4b8871968
http://kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.32.log
http://kernel.org/git/?p=linux/kernel/git/marcelo/linux-2.4.git;a=commit;h=2afb6d8ea04e81a1547e8e51b7550a8fd69b9fce

Other references:
http://secunia.com/advisories/17226/

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2005-3257

❖ 16056 Linux Kernel memory leak in "/security/keys/request_key_auth.c" to cause 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) and bypass certain security restrictions, or by malicious people to disclose certain sensitive information.

A memory leak in "/security/keys/request_key_auth.c" can potentially be exploited by non-privileged users to cause a DoS.

The vulnerability has been fixed in version 2.6.14-rc4 and stable version 2.6.13.4.

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

References:

Original advisory:
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=74fd92c511bd4a0771ac0faaaef38bb1be3a29f6
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=829841146878e082613a49581ae252c071057c23
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=9bc39bec87ee3e35897fe27441e979e7c208f624
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.14-rc4
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13.4
http://o0o.nu/~meder/o0o_linux_orinoco_driver_info_leak.txt
http://bugs.gentoo.org/show_bug.cgi?id=107893

Other references:
http://secunia.com/advisories/17114/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-3119, CAN-2005-3179, CAN-2005-3180, CAN-2005-3181

❖ 16057 Linux Kernel memory leak in "/fs/namei.c" to cause 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) and bypass certain security restrictions, or by malicious people to disclose certain sensitive information.

A memory leak exists in "/fs/namei.c" when the CONFIG_AUDITSYSCALL option is enabled. This can potentially be exploited by local users to cause a DoS via an excessive number of system calls.

The vulnerability has been fixed in version 2.6.14-rc4 and stable version 2.6.13.4.

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

References:

Original advisory:
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=74fd92c511bd4a0771ac0faaaef38bb1be3a29f6
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=829841146878e082613a49581ae252c071057c23
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=9bc39bec87ee3e35897fe27441e979e7c208f624
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.14-rc4
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13.4
http://o0o.nu/~meder/o0o_linux_orinoco_driver_info_leak.txt
http://bugs.gentoo.org/show_bug.cgi?id=107893

Other references:
http://secunia.com/advisories/17114/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-3119, CAN-2005-3179, CAN-2005-3180, CAN-2005-3181

❖ 16058 Linux Kernel orinoco wireless driver to expose random pieces of the system 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) and bypass certain security restrictions, or by malicious people to disclose certain sensitive information.

The orinoco wireless driver fails to pad data packets with zeroes when the length needs to be increased. This may cause uninitialized data to be sent, potentially exposing random pieces of the system memory.

The vulnerability has been fixed in version 2.6.14-rc4 and stable version 2.6.13.4

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

References:

Original advisory:
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=74fd92c511bd4a0771ac0faaaef38bb1be3a29f6
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=829841146878e082613a49581ae252c071057c23
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=9bc39bec87ee3e35897fe27441e979e7c208f624
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.14-rc4
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13.4
http://o0o.nu/~meder/o0o_linux_orinoco_driver_info_leak.txt
http://bugs.gentoo.org/show_bug.cgi?id=107893

Other references:
http://secunia.com/advisories/17114/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-3119, CAN-2005-3179, CAN-2005-3180, CAN-2005-3181

❖ 16059 Linux Kernel error in handling asynchronous USB access via usbdevio to crash kernel 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 handling asynchronous USB access via usbdevio can be exploited to crash the kernel via a process that issues an URB (USB Request Block) from userspace and terminates before the URB returns.

Successful exploitation requires that the user has permissions to access an USB device.

Vulnerability has been fixed in version 2.6.14.

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

References:

Original advisory:
http://marc.theaimsgroup.com/?l=linux-kernel&m=112766129313883
http://blog.blackdown.de/2005/05/09/fixing-the-ipt_recent-netfilter-module/
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.14
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.14.y.git;a=commit;h=46113830a18847cff8da73005e57bc49c2f95a56
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.14.y.git;a=commit;h=4ea6a8046bb49d43c950898f0cb4e1994ef6c89d
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174081

Other references:
http://secunia.com/advisories/16969/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2873, CAN-2005-3055, CVE-2005-3806

New Vulnerabilities found this Week

Symantec AntiVirus RAR Archive Decompression Buffer Overflow
"System access"

Alex Wheeler has reported a vulnerability in Symantec AntiVirus, which potentially can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in Dec2Rar.dll when copying data based on the length field in the sub-block headers of a RAR archive. This can be exploited to cause a heap-based buffer overflow and may allow arbitrary code execution when a malicious RAR archive is scanned.

The vulnerability has been reported in Dec2Rar.dll version 3.2.14.3 and potentially affects all Symantec products that use the DLL.

Solution:
Filter RAR archives at email or proxy gateways.

Provided and/or discovered by:
Alex Wheeler

Original Advisory:
http://www.rem0te.com/public/images/symc2.pdf

Microsoft Internet Explorer Multiple Vulnerabilities
“Security Bypass”

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.

This is related to:
SA16480

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.

For more information:
SA15546

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.

Solution:
Apply patches.

Internet Explorer 5.01 SP 4 on Microsoft Windows 2000 (requires SP 4):
http://www.microsoft.com/downloa...B74A-D6E6-4A32-A3B1-276686B4A428

Internet Explorer 6 SP 1 on Microsoft Windows 2000 (requires SP 4) or on Microsoft Windows XP (requires SP 1):
http://www.microsoft.com/downloa...3CD2-D98D-427B-9F0E-BD7E19FCB994

Internet Explorer 6 for Microsoft Windows XP (requires SP 2):

http://www.microsoft.com/downloa...BA57-D4F2-4798-9154-2869E371C9D1

Internet Explorer 6 for Microsoft Windows Server 2003 (with or without SP 1):
http://www.microsoft.com/downloa...FB20-C7C9-43AF-A864-6DBC9A542CC6

Internet Explorer 6 for Microsoft Windows Server 2003 (Itanium) (with or without SP 1):
http://www.microsoft.com/downloa...90B9-E596-4344-AEC3-FCB3289D7E9C

Internet Explorer 6 for Microsoft Windows Server 2003 x64 Edition:
http://www.microsoft.com/downloa...23E5-7988-42DA-A8BD-2C1A534BF995

Internet Explorer 6 for Microsoft Windows XP Professional x64 Edition:
http://www.microsoft.com/downloa...2B4A-6339-4B31-8ACF-D2A844C24F70

For Microsoft Windows 98, Microsoft Windows 98 SE, and Microsoft Windows Millennium Edition, see the vendors original advisory.

Provided and/or discovered by:
1) Andreas Sandblad, Secunia Research
2) Jakob Balle, Secunia Research
4) Will Dormann, CERT/CC

Original Advisory:
Secunia Research:
http://secunia.com/secunia_research/2005-7/advisory/
http://secunia.com/secunia_research/2005-21/advisory/

MS05-054 (KB905915):
http://www.microsoft.com/technet/security/Bulletin/MS05-054.mspx

Avaya Modular Messaging POP3 Denial of Service Vulnerability
"Denial of Service"

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

The vulnerability is caused due to an unspecified error in the POP3 service of the Message Storage Server. This can be exploited to cause a vulnerable service to enter an infinite loop by sending specially crafted packets.

Successful exploitation requires that the POP3 service is enabled (not enabled by default).

The vulnerability has been reported in version 2.0 Service Pack 4 and prior.

Solution:
Apply patch A1312pt+p.
http://support.avaya.com/elmodocs2/PSN/PSN599u.pdf

Provided and/or discovered by:
Reported by vendor.

Original Advisory:

Avaya:
http://support.avaya.com/elmodocs2/security/ASA-2005-235.pdf

PhpGedView File Inclusion and PHP Code Injection Vulnerabilities

"Exposure of sensitive information"

rgod has reported some vulnerabilities in PhpGedView, which can be exploited by malicious people to disclose sensitive information and compromise a vulnerable system.

1) Input passed to the "PGV_BASE_DIRECTORY" parameter in "help_text_vars.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources.

Successful exploitation requires that "register_globals" is enabled.

2) Input passed to the "user_language", "user_email", and "user_gedcomid" parameters when registering isn't properly sanitised before being stored in the PHP script "authenticate.php". This can be exploited to inject and execute arbitrary PHP code.

Successful exploitation requires that "magic_quotes_gpc" is disabled.

The vulnerabilities have been reported in version 3.3.7 and prior.

Solution:
Apply patch for version 3.3.7.
https://sourceforge.net/tracker/...p;group_id=55456&atid=477081

Provided and/or discovered by:
rgod

Original Advisory:
http://rgod.altervista.org/phpgedview_337_xpl.html

McAfee SecurityCenter "mcinsctl.dll" ActiveX File Overwrite Vulnerability

"Manipulation of data"

Peter Vreugdenhil has reported a vulnerability in McAfee SecurityCenter, which potentially can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an error in restricting the browser domain in which the "mcinsctl.dll" ActiveX control can be instantiated. The control contains the "MCINSTALL.McLog" object that can be used to write to a log file. This can be exploited to create or append to arbitrary files, potentially allowing arbitrary code execution by creating files in the user's startup folder.

Successful exploitation requires that the user is e.g. tricked into visiting a malicious website.

The vulnerability has been reported in "mcinsctl.dll" version 4.0.0.83 that is included with McAfee VirusScan. Other products that contain the vulnerability ActiveX control may also be affected.

Solution:
The vulnerability has reportedly been fixed via automatic update.

Provided and/or discovered by:
Peter Vreugdenhil

Changelog:
2005-12-21: Updated list of affected products.

Original Advisory:
iDEFENSE:
http://www.idefense.com/intellig...lnerabilities/display.php?id=358

HP-UX Software Distributor Unauthorised Access Vulnerability

"System access"

A vulnerability has been reported in HP-UX, which potentially can be exploited by malicious users to bypass certain security restrictions.

The vulnerability is caused due to an unspecified error in the Software Distributor (SD). This can be exploited by a remote user to gain unauthorized access.

The vulnerability has been reported in HP-UX B.11.11.

Solution:
Update to the fixed version.
http://itrc.hp.com

HP-UX B.11.11:
Install PHCO_33822 or later.

The vendor recommends using "swacl" to verify the SD Access Control Lists (ACLs) if IPv6 has ever been enabled prior to the installation of the recommended patch.

Provided and/or discovered by:
Reported by vendor.

Original Advisory:
HPSBUX02089 SSRT5983:
http://www2.itrc.hp.com/service/cki/docDisplay.do?docId=c00583199

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