ScoutNews Team **December 20, 2005**
Issue # 52

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

MS wmf zero-day cures emerging quickly, SONY close to settling DRM mess and predictions for the 2006 security outlook.

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

- **Microsoft zero-day exploit AV protection emerging**

Anti-Virus vendors are scrambling to publish signature files to respond to the plethora of attacks based on the Windows .wmf exploit that came out this week. Previously published workarounds endorsed by Microsoft can be problematic themselves.

Although dozens of variants have emerged in the last few days; AV vendors are quickly responding to the threat, some better than others.
eWeek

Full Story :
http://www.eweek.com/article2/0,1895,1907102,00.asp

- **Settlements discussed in SONY DRM lawsuit**

The settlement requires that Sony BMG will let consumers who bought the CDs receive replacement discs free from the anti-piracy technology and will offer two incentive packages.

The first includes a cash payment of $7.50 and a free download of one additional album from a list of more than 200 titles. The second package includes the download of three additional albums from the list. Apple iTunes could be one of the download services available.

Consumers who purchased MediaMax CDs would receive additional compensation.
Associated Press

Full Story:
http://www.kansas.com/mld/kansas/business/technology/13516456.htm

- **2006 predicted to bring Malware, flawed applications.**

2005 proved to be a good year for whitehats, we did a better job of blocking hackers and rolling out patches. Roger Grimes of InfoWorld predicts the storms for '06; he is foretelling more sophisticated malware and more application vulnerabilities. Good stuff.

Related Links:
http://www.infoworld.com/article/05/12/30/01OPsecadvise_1.html?9809798

New Vulnerabilities Tested in SecureScout

- **16060 Linux Kernel jiffies comparison in the "ipt_recent.c" netfilter module may cause ipt_recent netfilter rules to block too early 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 jiffies comparison in the "ipt_recent.c" netfilter module, when its value is greater than LONG_MAX, may cause ipt_recent netfilter rules to block too early.

Vulnerability has been fixed in version 2.6.14.

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

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

❖ 16061 Linux Kernel error in the IPv6 flowlabel handling code in "/net/ipv6/ip6_flowlabel.c" to cause the system to crash 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 IPv6 flowlabel handling code in "/net/ipv6/ip6_flowlabel.c" can be exploited by a local users to cause the kernel to free non-allocated memory. This corrupts kernel memory and can cause the system to crash.

Vulnerability has been fixed in version 2.6.14.

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

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

❖ 16062 Linux Kernel "fget()" Potential Denial of Service Vulnerability

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.

The vulnerability has been fixed in version 2.6.13.2.

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

References:

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

Other references:
http://secunia.com/advisories/16897/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-3044

❖ 16063 Linux Kernel boundary error in "sendmsg()" to allow malicious users to gain root privileges and execute arbitrary code Vulnerability

A vulnerability has been reported in the Linux kernel, which potentially can be exploited by malicious, local users to disclose certain sensitive information, cause a DoS (Denial of Service) and gain escalated privileges, or by malicious people to cause a DoS.

A boundary error in "sendmsg()" when copying 32bit "msg_control" contents from user-space to the kernel can be exploited to cause a buffer overflow. This may allow a malicious user to gain root privileges and execute arbitrary code with kernel privileges.

The vulnerability has been reported in version 2.6.9. Other versions may also be affected.

The vulnerability has been fixed in version 2.6.13.1.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13.1
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=166248
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=166249
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=166830

Other references:
http://secunia.com/advisories/16747/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2490, CAN-2005-2492, CVE-2005-3753

❖ 16064 Linux Kernel error in the "raw_sendmsg()" to disclose kernel memory contents or to manipulate certain hardware state to cause a Denial of Service Vulnerability

A vulnerability has been reported in the Linux kernel, which potentially can be exploited by malicious, local users to disclose certain sensitive information, cause a DoS (Denial of Service) and gain escalated privileges, or by malicious people to cause a DoS.

An error in the "raw_sendmsg()" function may allow a malicious user to read kernel memory contents and disclose certain information, or to manipulate certain hardware state to cause a DoS.

The vulnerability has been fixed in version 2.6.13.1.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13.1
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=166248
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=166249
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=166830

Other references:
http://secunia.com/advisories/16747/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2490, CAN-2005-2492, CVE-2005-3753

❖ 16065 Linux Kernel error in performing boundary checks in the standard multi-block cipher processors to cause a kernel panic Vulnerability

A vulnerability has been reported in the Linux kernel, which potentially can be exploited by malicious, local users to disclose certain sensitive information, cause a DoS (Denial of Service) and gain escalated privileges, or by malicious people to cause a DoS.

An error in performing boundary checks in the standard multi-block cipher processors can be exploited to cause a kernel panic in an IPSec environment when handling packets with a block size that is not multiple of "bsize".

The vulnerability has been fixed in version 2.6.13.1.

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

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13.1
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=166248
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=166249
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=166830

Other references:
http://secunia.com/advisories/16747/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2490, CAN-2005-2492, CVE-2005-3753

❖ 16066 Linux Kernel "setsockopt()" function not restricted to privileged users leads to bypass IPsec policies or exhaust available kernel memory 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), disclose potentially sensitive information, and bypass certain security restrictions, or by malicious people to cause a DoS.

The "setsockopt()" function is not restricted to privileged users with the "CAP_NET_ADMIN" capability. This can be exploited to bypass IPsec policies or set invalid policies to exploit other vulnerabilities or exhaust available kernel memory.

The vulnerability has been fixed in version 2.6.13.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=d04b4f8c1c9766e49fad6a141fc61cb30db69a5c
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-

2.6.13.y.git;a=commit;h=fb3d89498d268c8dedc1ab5b15fa64f536564577
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=71ae18ec690953e9ba7107c7cc44589c2cc0d9f1
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=cb94c62c252796f42bb83fe40960d12f3ea5a82a
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=bfd272b1ca1164382eabaa9986aad822adb91eb2
http://www.kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.32
http://www.kernel.org/git/?p=linux/kernel/git/marcelo/linux-2.4.git;a=commit;h=e684f066dff5628bb61ad1912de6e8058b5b4c7d
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174345
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174344

Other references:
http://secunia.com/advisories/16494/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2555, CAN-2005-2617, CAN-2005-2800, CAN-2005-3053, CVE-2005-3274, CVE-2005-3275, CVE-2005-3276, CVE-2005-3848, CVE-2005-3858

❖ 16067 Linux Kernel error in "syscall32_setup_pages()" to cause a memory leak 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), disclose potentially sensitive information, and bypass certain security restrictions, or by malicious people to cause a DoS.

An error in the "syscall32_setup_pages()" function on 64-bit x86 platforms can be exploited to cause a memory leak by executing a malicious 32-bit application with specially crafted ELF headers.

The vulnerability has been fixed in version 2.6.13.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=d04b4f8c1c9766e49fad6a141fc61cb30db69a5c
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=fb3d89498d268c8dedc1ab5b15fa64f536564577
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=71ae18ec690953e9ba7107c7cc44589c2cc0d9f1
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=cb94c62c252796f42bb83fe40960d12f3ea5a82a
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=bfd272b1ca1164382eabaa9986aad822adb91eb2
http://www.kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.32

http://www.kernel.org/git/?p=linux/kernel/git/marcelo/linux-2.4.git;a=commit;h=e684f066dff5628bb61ad1912de6e8058b5b4c7d
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174345
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174344

Other references:
http://secunia.com/advisories/16494/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2555, CAN-2005-2617, CAN-2005-2800, CAN-2005-3053, CVE-2005-3274, CVE-2005-3275, CVE-2005-3276, CVE-2005-3848, CVE-2005-3858

❖ 16068 Linux Kernel error in seq_file implementation to cause a memory leak 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), disclose potentially sensitive information, and bypass certain security restrictions, or by malicious people to cause a DoS.

An error in seq_file implementation in the SCSI procfs interface (sg.c), can be exploited to cause a memory leak by repeatedly reading from the /proc/scsi/sg/devices file.

The vulnerability has been fixed in version 2.6.13.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=d04b4f8c1c9766e49fad6a141fc61cb30db69a5c
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=fb3d89498d268c8dedc1ab5b15fa64f536564577
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=71ae18ec690953e9ba7107c7cc44589c2cc0d9f1
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=cb94c62c252796f42bb83fe40960d12f3ea5a82a
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=bfd272b1ca1164382eabaa9986aad822adb91eb2
http://www.kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.32
http://www.kernel.org/git/?p=linux/kernel/git/marcelo/linux-2.4.git;a=commit;h=e684f066dff5628bb61ad1912de6e8058b5b4c7d
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174345
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174344

Other references:
http://secunia.com/advisories/16494/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2555, CAN-2005-2617, CAN-2005-2800, CAN-2005-3053, CVE-2005-3274, CVE-2005-3275, CVE-2005-3276, CVE-2005-3848, CVE-2005-3858

❖ 16069 Linux Kernel error in validating the first argument of "sys_set_mempolicy()" to cause a 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), disclose potentially sensitive information, and bypass certain security restrictions, or by malicious people to cause a DoS.

An error in validating the first argument of the "sys_set_mempolicy()" function in "mm/mempolicy.c" may be exploited to cause a DoS via a negative argument value.

The vulnerability has been fixed in version 2.6.13.

Test Case Impact: **xxxxxxxx** Vulnerability Impact: **xxxxxx** Risk: **xxxxxx**

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=d04b4f8c1c9766e49fad6a141fc61cb30db69a5c
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=fb3d89498d268c8dedc1ab5b15fa64f536564577
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=71ae18ec690953e9ba7107c7cc44589c2cc0d9f1
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=cb94c62c252796f42bb83fe40960d12f3ea5a82a
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.13.y.git;a=commit;h=bfd272b1ca1164382eabaa9986aad822adb91eb2
http://www.kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.32
http://www.kernel.org/git/?p=linux/kernel/git/marcelo/linux-2.4.git;a=commit;h=e684f066dff5628bb61ad1912de6e8058b5b4c7d
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174345
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174344

Other references:
http://secunia.com/advisories/16494/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-2555, CAN-2005-2617, CAN-2005-2800, CAN-2005-3053, CVE-2005-3274, CVE-2005-3275, CVE-2005-3276, CVE-2005-3848, CVE-2005-3858

New Vulnerabilities found this Week

Microsoft Windows WMF "SETABORTPROC" Arbitrary Code Execution
"Execute arbitrary code"

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

The vulnerability is caused due to an error in the handling of Windows Metafile files (".wmf") containing specially crafted SETABORTPROC "Escape" records. Such records allow arbitrary user-defined function to be executed when the rendering of a WMF file fails. This can be exploited to execute arbitrary code by tricking a user into opening a malicious ".wmf" file in "Windows Picture and Fax Viewer" or previewing a malicious ".wmf" file in explorer (i.e. opening a folder containing a malicious image file).

The vulnerability can also be exploited automatically when a user visits a malicious web site using Microsoft Internet Explorer.

NOTE: Exploit code is publicly available. This is being exploited in the wild. The vulnerability can also be triggered from explorer if the malicious file has been saved to a folder and renamed to other image file extensions like ".jpg", ".gif, ".tif", and ".png" etc.

The vulnerability has been confirmed on a fully patched system running Microsoft Windows XP SP2. Microsoft Windows XP SP1 and Microsoft Windows Server 2003 SP0 / SP1 are reportedly also affected. Other platforms may also be affected.

Solution:
Do not save, open or preview untrusted image files from email or other sources, or open untrusted folders and network shares in explorer.

Set security level to "High" in Microsoft Internet Explorer to prevent automatic exploitation.

The risks can be mitigated by unregistering "Shimgvw.dll". However, this will disable certain functionalities. Secunia do not recommend the use of this workaround on production systems until it has been thoroughly tested.

Provided and/or discovered by:
First reported in the wild by "noemailpls".

Exploit code and additional information provided by H D Moore.

References:
Microsoft (KB912840):
http://www.microsoft.com/technet/security/advisory/912840.mspx
US-CERT VU#181038: http://www.kb.cert.org/vuls/id/181038
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4560
http://www.frsirt.com/english/advisories/2005/3086
http://www.frsirt.com/exploits/20051228.ie_xp_pfv_metafile.pm.php

dtSearch DUNZIP32.dll Buffer Overflow Vulnerability

“system access”

uha-Matti Laurio has reported a vulnerability in dtSearch, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in a 3rd-party compression library (DUNZIP32.dll) when extracting a ZIP file.

Successful exploitation requires that the user is e.g. tricked into indexing a malicious ZIP file.

The vulnerability has been reported in versions prior to 7.20.

Solution:
Update to version 7.20 Build 7136.
http://www.dtsearch.com/download.html#upgrades

Provided and/or discovered by:
Juha-Matti Laurio

Original Advisory:
http://www.networksecurity.fi/advisories/dtsearch.html

PHPSurveyor "sid" SQL Injection Vulnerability
“Data Manipulation”

taqua has reported a vulnerability in PHPSurveyor, which can be exploited by malicious people to conduct SQL injection attacks.

Input passed to the "sid" parameter isn't properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

The vulnerability has been reported in version 0.99. Prior versions may also be affected.

Solution:
Update to version 0.991:
http://sourceforge.net/project/showfiles.php?group_id=74605

Provided and/or discovered by:
taqua

VisNetic Mail Server Multiple Webmail Vulnerabilities
“Exposure of sensitive information, System access”

Secunia Research has discovered some vulnerabilities in VisNetic Mail Server, which can be exploited by malicious users and by malicious people to disclose potentially sensitive information and to compromise a vulnerable system.

1) The webmail and webadmin services run with PHP configured with "register_global" enabled. The "language" and "lang_settings" variables in "/accounts/inc/include.php" and "/admin/inc/include.php" are not properly initialised when the scripts are

accessed directly. This makes it possible to overwrite the variables to cause the scripts to include arbitrary PHP scripts from local and remote sources.

Example:
http://[host]:32000/accounts/inc/include.php?language=0&lang_settings[0][1]=http://[host]/
http://[host]:32000/admin/inc/include.php?language=0&lang_settings[0][1]=http://[host]/

Successful exploitation allows execution of arbitrary PHP code on a vulnerable server with SYSTEM privileges without requiring authentication.

2) Input passed to the "lang" parameter in "/dir/include.html" isn't properly validated before being used to include files. This can be exploited to include arbitrary files from local sources.

Example:
http://[host]:32000/dir/include.html?lang=[file]%00

Successful exploitation allows disclosure of arbitrary files on a vulnerable server without requiring authentication.

3) Input passed to the "language" parameter in "/mail/settings.html" isn't properly validated before being saved to the database. This can be exploited in conjunction with overwrite of the "lang_settings" variable, to include arbitrary PHP scripts from local and remote sources.

Example:
http://[host]:32000/mail/settings.html?id=[current_id]&Save_x=1&language=TEST
http://[host]:32000/mail/index.html?id=[current_id]&lang_settings[TEST]=test;http://[host]/;

Successful exploitation allows execution of arbitrary PHP scripts on a vulnerable server with SYSTEM privileges but requires a valid logon.

4) The "default_layout" and "layout_settings" variables are not properly initialised when "/mail/include.html" encounters a HTTP_USER_AGENT string that it does not recognise. This can be exploited in conjunction with overwrite of the "default_layout" and "layout_settings" variables to disclose the content of local files.

Example (using non-IE/Mozilla/Firefox browser):
http://[host]:32000/mail/index.html?/mail/index.html?default_layout=OUTLOOK2003&layout_settings[OUTLOOK2003]=test;[file]%00;2

Successful exploitation allows disclosure of arbitrary files on a vulnerable server without requiring authentication.

The vulnerabilities have been confirmed in version 8.3.0 build 1 General Availability Release [2005-12-02]. Prior versions may also be affected.

Solution:
Update to version 8.3.5: http://www.deerfield.com/download/visnetic-mailserver/

Provided and/or discovered by:
Tan Chew Keong, Secunia Research.

Original Advisory:
Secunia Research: http://secunia.com/secunia_research/2005-62/advisory/

Golden FTP Server APPE Command Buffer Overflow
"System access"

Tim Shelton has discovered a vulnerability in Golden FTP Server, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the handling of the "APPE" FTP command. This can be exploited to cause a buffer overflow by supplying an overly long argument.

The vulnerability has been confirmed in version 1.92. Other versions may also be affected.

Solution:
Use the product only when connected to trusted networks.

Provided and/or discovered by:
Tim Shelton

Proxim Wireless Access Points Static WEP Key Authentication Bypass
"Security Bypass"

Urmas Kahar and Tarmo Kaljumae have reported a security issue in Proxim Wireless Access Points products, which can be exploited by malicious people to bypass certain security restrictions.

The problem is caused due to the presence of a static WEP key set to "12345". This can be exploited to bypass the 802.1x authentication and gain access to network resources.

Successful exploitation requires that the access point has 802.1x enabled and WEP disabled.

The following products are affected:
* Proxim Wireless Access Points AP-600 and AP-2000 (all versions after 2.4.11 and prior to 2.5.5)
* Proxim Wireless Access Points AP-700 and AP-4000 (all versions after 2.4.11 and prior to 3.1)

Solution:
Proxim Wireless Access Points AP-600:
Apply firmware 2.5.5.
http://support.proxim.com/cgi-bi...enduser/std_adp.php?p_faqid=1222

Proxim Wireless Access Points AP-2000:
Apply firmware 2.5.5.
http://support.proxim.com/cgi-bi...enduser/std_adp.php?p_faqid=1221

Proxim Wireless Access Points AP-700:

Apply firmware 3.1.
http://support.proxim.com/cgi-bi...enduser/std_adp.php?p_faqid=1686

Proxim Wireless Access Points AP-4000:
Apply firmware 3.1.
http://support.proxim.com/cgi-bi...enduser/std_adp.php?p_faqid=1250

Provided and/or discovered by:
Urmas Kahar and Tarmo Kaljumae

Original Advisory:
http://keygen.proxim.com/support/cs/Documents/802.1x_vulnerability.pdf

DEV web management system Cross-Site Scripting and SQL Injection
"XSS, SQL Injection"

rgod has reported some vulnerabilities in DEV web management system, which can be exploited by malicious people to conduct cross-site scripting and SQL injection attacks.

1) Input passed to the "cat" parameter in "index.php" and "getfile.php", and the "target" parameter in "download_now.php" isn't properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

Examples:
http://[host]/index.php?session=0&action=openforum&cat=[code]
http://[host]/getfile.php?cat=[code]
http://[host]/download_now.php?target=[code]

2) Input passed to the "language" array parameter in "add.php" 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.

Examples:
http://[host]/add.php?language[ENTER_ARTICLE_TITLE]=[code]
http://[host]/add.php?language[SPECIFY_ZONE]=[code]
http://[host]/add.php?language[ENTER_ARTICLE_HEADER]=[code]
http://[host]/add.php?language[ENTER_ARTICLE_BODY]=[code]

The vulnerabilities have been reported in version 1.5 and prior. Other versions may also be affected.

Solution:
Edit the source code to ensure that input is properly sanitised.

Provided and/or discovered by:
rgod

Original Advisory:
http://rgod.altervista.org/dev_15_sql_xpl.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