netVigilance

ScoutNews Team

January 6, 2006
2006 Issue # 12

Weekly ScoutNews by netVigilance

Table of Contents

Product Focus - SecureScout Perimeter

Extend your Scanning capabilities to your internet-facing IP addresses with SecureScout Perimeter.

With remote scanning agents, you can user Perimeter to scan internal and external IPs and generate a single report for your entire network.

This Week in Review

SecureTest is vigilant on lost password sites, Students in Florida get A's in computer security, 'Perfect Storm' of IT surveys too perfect and the Missile Defense Agency leaves the back door open.

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

- **SecureTest warns that lost password site can be a risk**

SecureTest finds that 50.5 per cent of 107 e-commerce website tested were vulnerable to enumeration attacks. Hackers flood lost password pages with usernames until they get hits on any that don't return an "invalid user name" message.

Once the hacker has this list, they use similar methods to crack the passwords.

The Register

Full Story :
http://www.channelregister.co.uk/2006/03/20/forgotten_password_security_risk/

- ### Palm Beach County Schools report hackers altered grades

School officials and Police suspect that students were responsible for breaking in to the School District's computer system and altering grades.

These altered grades may have had an effect on college entrance applications as well. (Maybe start with the kids that Aced computer technology AND poetry – Ed.)

South Florida Sun-Sentinel

Full Story :

http://www.sun-sentinel.com/news/education/sfl-pgrades22mar22,0,1399484.story

- ### Network World finds subjectivity in recent surveys

Network World found that 20 leading security vendors published 34 surveys which were conducted by third parties on behalf. Most of the surveys made attempts to escalate certain security threats that were in the sweet spot for these vendors solutions (surprise!)

With the flurry of surveys warning that the sky is falling, care needs to be taken to sort out the realistic results.

Tech World

Full Story :

http://www.techworld.com/security/features/index.cfm?FeatureID=2350

- ### US Missile Defense system left open

An audit of the Missile Defense Agency (MDA) and Prime contractor Boeing finds very serious security flaws in the Ground-based Midcourse Defense (GMD) system and the GMD Communications Network (GCN). The system was built to conform to 20 year-old DOD guidelines rather that 21st century rules. Some of the lax 'security' measures include the use of group passwords on the unencrypted portion of the GCN as opposed to individual passwords and lack of backup contingency plans.

Apparently the systems were rushed forward to protect the US from ICBM attacks from Asia.

"*We have met the enemy and he is us*" - Pogo

FCW

Related Links :
http://www.fcw.com/article92665-03-20-06-Print

New Vulnerabilities Tested in SecureScout

- **16170 Microsoft Internet Explorer "createTextRange()" Code Execution (Remote File Checking)**

Secunia Research has discovered a vulnerability in Microsoft Internet Explorer, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error in the processing of the "createTextRange()" method call applied on a radio button control. This can be exploited by e.g. a malicious web site to corrupt memory in a way, which allows the program flow to be redirected to the heap.

Successful exploitation allows execution of arbitrary code.

The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2. The vulnerability has also been confirmed in Internet Explorer 7 Beta 2 Preview (January edition). Other versions may also be affected

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

References:

Original advisory:
http://secunia.com/secunia_research/2006-7/

Other references:
Microsoft Security Response Center Blog:
http://blogs.technet.com/msrc/archive/2006/03/22/422849.aspx
US-CERT VU#876678:
http://www.kb.cert.org/vuls/id/876678
MSDN:
http://msdn.microsoft.com/workshop/author/dhtml/reference/methods/createtextrange.asp

CVE Reference: None

❖ 16171 Sendmail Signal Handling Memory Corruption Vulnerability

ISS X-Force has reported a vulnerability in Sendmail, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a signal handling error when receiving and processing mail data from clients. This can be exploited to corrupt memory by sending specially crafted data at certain time intervals.

Successful exploitation allows execution of arbitrary code with the privileges of the sendmail server daemon.

The issue has been fixed in Sendmail version 8.13.6.

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

References:

Original Advisory:
* ISS:20060322 Sendmail Remote Signal Handling Vulnerability
http://xforce.iss.net/xforce/alerts/id/216

Other References:
* REDHAT:RHSA-2006:0264
* URL:http://www.redhat.com/support/errata/RHSA-2006-0264.html
* REDHAT:RHSA-2006:0265
* URL:http://www.redhat.com/support/errata/RHSA-2006-0265.html
* CERT:TA06-081A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-081A.html
* CERT-VN:VU#834865
* URL:http://www.kb.cert.org/vuls/id/834865
* FRSIRT:ADV-2006-1049
* URL:http://www.frsirt.com/english/advisories/2006/1049
* FRSIRT:ADV-2006-1051
* URL:http://www.frsirt.com/english/advisories/2006/1051

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

CVE Reference: CVE-2006-0058

❖ 16172 RealPlayer (10.5/10.5 Beta/10/8) / RealOne Player (v2/v1) boundary error when processing SWF files (Remote File Checking

A vulnerability has been reported in various RealNetworks products, which can be exploited by malicious people to compromise a user's system.

A boundary error when processing SWF files can be exploited to cause a buffer overflow. This may allow execution of arbitrary code on the user's system.

The following products are affected:
* RealPlayer 10.5 (6.0.12.1040-1348)
* RealPlayer 10

* RealOne Player v2
* RealOne Player v1
* RealPlayer 8
* RealPlayer Enterprise
* Rhapsody 3 (build 0.815 1.0.269)
* Mac RealPlayer 10 (10.0.0.305 - 331)
* Mac RealOne Player
* Linux RealPlayer 10 (10.0.6)
* Helix Player (10.0.6)
* Linux RealPlayer 10 (10.0.0 - 5)
* Helix Player (10.0.0 - 5)

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

References:

Original Advisories:
RealNetworks:
http://service.real.com/realplayer/security/03162006_player/en/

Other references:
http://secunia.com/advisories/19358/

Product HomePage:
http://service.real.com/realplayer/security/

CVE Reference: CAN-2005-2936, CVE-2006-0323, CAN-2005-2922

❖ 16173 RealPlayer (10.5/10.5 Beta/10/8) / RealOne Player (v2/v1) boundary error within the handling of web pages (Remote File Checking)

A vulnerability has been reported in various RealNetworks products, which can be exploited by malicious people to compromise a user's system.

A boundary error within the handling of web pages can be exploited via a specially crafted web page on a malicious server to cause a heap-based buffer overflow. This may allow execution of arbitrary code on the user's system.

The following products are affected:
* RealPlayer 10.5 (6.0.12.1040-1348)
* RealPlayer 10
* RealOne Player v2
* RealOne Player v1
* RealPlayer 8
* RealPlayer Enterprise
* Rhapsody 3 (build 0.815 1.0.269)
* Mac RealPlayer 10 (10.0.0.305 - 331)
* Mac RealOne Player
* Linux RealPlayer 10 (10.0.6)
* Helix Player (10.0.6)
* Linux RealPlayer 10 (10.0.0 - 5)
* Helix Player (10.0.0 - 5)

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

References:

Original Advisories:
RealNetworks:
http://service.real.com/realplayer/security/03162006_player/en/

Other references:
http://secunia.com/advisories/19358/

Product HomePage:
http://service.real.com/realplayer/security/

CVE Reference: CAN-2005-2936, CVE-2006-0323, CAN-2005-2922

❖ 16174 RealPlayer (10.5/10.5 Beta/10/8) / RealOne Player (v2/v1) boundary error in the processing of MBC files (Remote File Checking)

A vulnerability has been reported in various RealNetworks products, which can be exploited by malicious people to compromise a user's system.

A boundary error in the processing of MBC files can be exploited to cause a buffer overflow. This may allow execution of arbitrary code on the user's system.

The following products are affected:
* RealPlayer 10.5 (6.0.12.1040-1348)
* RealPlayer 10
* RealOne Player v2
* RealOne Player v1
* RealPlayer 8
* RealPlayer Enterprise
* Rhapsody 3 (build 0.815 1.0.269)
* Mac RealPlayer 10 (10.0.0.305 - 331)
* Mac RealOne Player
* Linux RealPlayer 10 (10.0.6)
* Helix Player (10.0.6)
* Linux RealPlayer 10 (10.0.0 - 5)
* Helix Player (10.0.0 - 5)

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

References:

Original Advisories:

RealNetworks:

http://service.real.com/realplayer/security/03162006_player/en/

Other references:

http://secunia.com/advisories/19358/

Product HomePage:

http://service.real.com/realplayer/security/

CVE Reference: CAN-2005-2936, CVE-2006-0323, CAN-2005-2922

❖ 16175 RealPlayer (10.5/10.5 Beta/10/8) / RealOne Player (v2/v1) incorrect use of the "CreateProcess()" API (Remote File Checking)

A weakness when executing other programs is caused due to incorrect use of the "CreateProcess()" API. This may allow execution of an arbitrary program on the system, if this can be placed in the program path.

The following products are affected:
* RealPlayer 10.5 (6.0.12.1040-1348)
* RealPlayer 10
* RealOne Player v2
* RealOne Player v1
* RealPlayer 8
* RealPlayer Enterprise
* Rhapsody 3 (build 0.815 1.0.269)
* Mac RealPlayer 10 (10.0.0.305 - 331)
* Mac RealOne Player
* Linux RealPlayer 10 (10.0.6)
* Helix Player (10.0.6)
* Linux RealPlayer 10 (10.0.0 - 5)
* Helix Player (10.0.0 - 5)

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

References:

Original Advisories:
RealNetworks:
http://service.real.com/realplayer/security/03162006_player/en/

Other references:
http://secunia.com/advisories/19358/

Product HomePage:
http://service.real.com/realplayer/security/

CVE Reference: CAN-2005-2936, CVE-2006-0323, CAN-2005-2922

❖ 16176 Linux Kernel "sockaddr_in.sin_zero" Information Disclosure

Pavel Kankovsky has reported a weakness in the Linux kernel, which can be exploited by malicious, local users to disclose potentially sensitive information.

The weakness is caused due to the "sockaddr_in.sin_zero" array not being zeroed before being returned to user space programs calling certain socket functions to retrieve information about the specified socket. This can be exploited to disclose six uninitialised bytes of the kernel stack via calls to the "getsockopt()" function with the "SO_ORIGINAL_DST" option, or via calls to the "getsockname()", "getpeername()", and "accept()" functions.

The weakness has been reported in the 2.4 and 2.6 kernel branches.

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

References:

Original advisory:
http://marc.theaimsgroup.com/?l=linux-netdev&m=114148078223594&w=2

Other references:
http://www.kernel.org/git/?p=linux/kernel/git/marcelo/linux-2.4.git;a=commit;h=09d3b3dcfa80c9094f1748c1be064b9326c9ef2b

Product HomePage:
http://kernel.org/

CVE Reference: CVE-2006-1342, CVE-2006-1343

❖ 16177 Linux Kernel Netfilter Vulnerability

A Vulnerability has been reported in the Linux Kernel with an unknown impact.

An integer overflow error exists within the "do_replace()" function in Netfilter. This can be exploited to cause a buffer overflow and allows the overwrite of arbitrary amounts of kernel memory when data is copied from user space.

Successful exploitation requires that the user is granted CAP_NET_ADMIN rights e.g. on systems that uses certain virtualisation solutions such as OpenVZ.

Vulnerability has been fixed in version 2.6.16.

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

References:

Original advisory:
* BID:17178
* http://www.securityfocus.com/bid/17178

Other references:
http://secunia.com/advisories/19330/
* CONFIRM:https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=186295
* CONFIRM:http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=ee4bb818ae35f68d1f848eae0a7b150a38eb4168

Product HomePage:

http://kernel.org/

CVE Reference: CVE-2006-0038

❖ 16178 Linux Kernel handling of NDIS response to cause kernel memory corruption

A vulnerability has been reported in the Linux Kernel with an unknown impact.

Insufficient memory allocation in "drivers/usb/gadget/rndis.c" when handling NDIS response to OID_GEN_SUPPORTED_LIST may cause kernel memory corruption.

Vulnerability has been fixed in version 2.6.16.

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

References:

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

Other references:
http://secunia.com/advisories/19330/
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=ee4bb818ae35f68d1f848eae0a7b150a38eb4168
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=8763716bfe4d8a16bef28c9947cf9d799b1796a5

Product HomePage:
http://kernel.org/

CVE Reference: None

❖ 16179 avast! Antivirus Insecure Default File Permissions (Remote File Checking)

A security issue has been reported in avast! Antivirus, which can be exploited by malicious, local users to bypass certain security restrictions or gain escalated privileges.

The security issue is caused due to insecure default file permissions being set on the installed files and folders. This allows any non-privileged users on the system to remove the files or replace them with malicious binaries.

Successful exploitation reportedly requires that the TEMP folder is on the same drive as the avast! installation folder.

The security issue has been confirmed in avast! Professional Edition version 4.6.763 with database 612-0 and also reported in the Home Edition. Other versions may also be affected.

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

References:

Original Advisory:

http://forum.avast.com/index.php?topic=19862.0

Product HomePage:

http://www.dslreports.com/forum/remark,15601404~days=9999~start=20

Other references:

http://secunia.com/advisories/19284/

CVE Reference: None

New Vulnerabilities found this Week

Microsoft Internet Explorer "createTextRange()" Code Execution
“Execution of arbitrary code”

Secunia Research has discovered a vulnerability in Microsoft Internet Explorer, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error in the processing of the "createTextRange()" method call applied on a radio button control. This can be exploited by e.g. a malicious web site to corrupt memory in a way, which allows the program flow to be redirected to the heap.

Successful exploitation allows execution of arbitrary code.

NOTE: Exploit code is publicly available.

The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2. The vulnerability has also been confirmed in Internet Explorer 7 Beta 2 Preview (January edition). Other versions may also be affected.

References:
http://descriptions.securescout.com/tc/16170
http://secunia.com/secunia_research/2006-7/
http://www.kb.cert.org/vuls/id/876678
http://blogs.technet.com/msrc/archive/2006/03/22/422849.aspx

Sendmail Signal Handling Memory Corruption Vulnerability
“Execution of arbitrary code”

ISS X-Force has reported a vulnerability in Sendmail, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a signal handling error when receiving and processing mail data from clients. This can be exploited to corrupt memory by sending specially crafted data at certain time intervals.

Successful exploitation allows execution of arbitrary code with the privileges of the sendmail server daemon.

The vulnerability has been reported in the following products:
* Sendmail 8.13.5 and prior
* Sendmail 8.12.11 and prior
* Sendmail Sentrion 1.1
* Sendmail Switch 2.x, 3.0.x, and 3.1.x (Solaris, Linux, AIX, and HP-UX)
* Sendmail Managed MTA 2.x, 3.0.x, and 3.1.x (Solaris, Linux, AIX, and HP-UX)
* Sendmail Multi-Switch 2.x, 3.0.x, and 3.1.x (Solaris, Linux, AIX, and HP-UX)
* Sendmail Message Store/SAMS 1.2.x, 2.0.x, 2.1.x, and 2.2.x (Solaris, Linux, AIX, and HP-UX)
* Intelligent Quarantine 3.0 (Solaris or Linux)

References:
http://descriptions.securescout.com/tc/16171
http://xforce.iss.net/xforce/alerts/id/216
http://www.sendmail.org/8.13.6.html
http://www.kb.cert.org/vuls/id/834865

Linux Kernel IPv4 "sockaddr_in.sin_zero" Information Disclosure
“Disclose potentially sensitive information”

Pavel Kankovsky has reported a weakness in the Linux kernel, which can be exploited by malicious, local users to disclose potentially sensitive information.

The weakness is caused due to the "sockaddr_in.sin_zero" array not being zeroed before being returned to user space programs calling certain socket functions to retrieve information about the specified socket. This can be exploited to disclose six uninitialised bytes of the kernel stack via calls to the "getsockopt()" function with the "SO_ORIGINAL_DST" option, or via calls to the "getsockname()", "getpeername()", and "accept()" functions.

The weakness has been reported in the 2.4 and 2.6 kernel branches.

NOTE: The weakness in the "getsockname()", "getpeername()", and "accept()" functions affect only the 2.4 kernel.

References:
http://descriptions.securescout.com/tc/16176
http://marc.theaimsgroup.com/?l=linux-netdev&m=114148078223594&w=2
http://www.kernel.org/git/?p=linux/kernel/git/marcelo/linux-2.4.git;a=commit;h=09d3b3dcfa80c9094f1748c1be064b9326c9ef2b

Linux Kernel Netfilter Weakness and RNDIS Buffer Overflow
“Integer overflow; kernel memory corruption”

A weakness and a vulnerability have been reported in the Linux Kernel, which have unknown impacts.

1) An integer overflow error exists within the "do_replace()" function in Netfilter. This can be exploited to cause a buffer overflow and allows overwriting of arbitrary amounts of kernel memory when data is copied from user space.

Successful exploitation requires that the user is granted CAP_NET_ADMIN rights e.g. on systems that uses certain virtualisation solutions such as OpenVZ.

2) Insufficient memory allocation in "drivers/usb/gadget/rndis.c" when handling NDIS response to OID_GEN_SUPPORTED_LIST may cause kernel memory corruption.

References:
http://descriptions.securescout.com/tc/16177
http://descriptions.securescout.com/tc/16178
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16

avast! Antivirus Insecure Default File Permissions
“Bypass certain security restrictions or gain escalated privileges”

A security issue has been reported in avast! Antivirus, which can be exploited by malicious, local users to bypass certain security restrictions or gain escalated privileges.

The security issue is caused due to insecure default file permissions being set on the installed files and folders. This allows any non-privileged users on the system to remove the files or replace them with malicious binaries.

Successful exploitation reportedly requires that the TEMP folder is on the same drive as the avast! Installation folder.

The security issue has been confirmed in avast! Professional Edition version 4.6.763 with database 612-0 and also reported in the Home Edition. Other versions may also be affected.

References:
http://descriptions.securescout.com/tc/16179
http://forum.avast.com/index.php?topic=19862.0
http://www.dslreports.com/forum/remark,15601404~days=9999~start=20

VERITAS Backup Exec Denial of Service and Format String Vulnerabilities
“Denial of Service”

Some vulnerabilities have been reported in VERITAS Backup Exec, which can be exploited by malicious users to cause a DoS and potentially to compromise a vulnerable system, and by malicious people to cause a DoS (Denial of Service).

1) Some errors exist within the Backup Exec Remote Agent when handling certain received malformed packets. This can be exploited to cause memory access violations or exhaust system resources, thus causing the service to crash or stop responding until it is restarted.

Successful exploitation causes DoS of the backup functionality.

The vulnerabilities have been reported in the following products:

* Backup Exec 9.2 for NetWare Servers - All Agents (Netware, Windows, & Linux/Unix).
* Backup Exec 9.1 for NetWare Servers - All Agents (NetWare, Windows, & Linux/Unix).
* Backup Exec 10d (10.1) for Windows Servers rev. 5629 - All Remote Agents (RAWS, RANW, & RALUS)
* Backup Exec 10.0 for Windows Servers rev. 5520 - All Remote Agents (RAWS, RANW, & RALUS)
* Backup Exec 10.0 for Windows Servers rev. 5484 - All Remote Agents (RAWS, RANW, & RALUS)
* Backup Exec 9.1 for Windows Servers rev. 4691 - Remote Agent for Windows Servers (RAWS)

2) A format string error exists within the job logging functionality of Backup Exec for Windows. This can be exploited to cause a DoS and may allow arbitrary code execution when a file with specially-crafted filename is backed up.

Successful exploitation requires that job logging is configured with "full details" enabled (non-default), and that a malicious user is able to create a file with specially-crafted filename on a system that is backed up.

The vulnerability has been reported in the following products:
* Backup Exec 10d (10.1) for Windows Servers rev. 5629
* Backup Exec 10.0 for Windows Servers rev. 5520
* Backup Exec 10.0 for Windows Servers rev. 5484
* Backup Exec 9.1 for Windows Servers rev. 4691

References:
http://securityresponse.symantec.com/avcenter/security/Content/2006.03.17a.html
http://securityresponse.symantec.com/avcenter/security/Content/2006.03.17b.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