netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 18 May 5, 2006

Table of Contents

Product Focus

Mydoom Worm Scanner – Scan up to 256 IP addresses for MyDoom variants with this free scanner available on netvigilance.com.

This Week in Review

RFID makes hacking easier, Apple makes the SANS Top 20 for first time and the perils of patching?

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

- **RFID creating mother-lode for Hackers**

Annalee Newitz at Wired gives an entertaining expose on the relative ease at which RFID data can be hacked. With the future boding such applications as ID in US passports, credit cards and the medical industry is exploring the use of implantable chips for patients; personal data could be exposed to hacking by a 'casual brush' as the vignette in the article demonstrates.

Wired

Full Story :
http://www.wired.com/wired/archive/14.05/rfid.html

- **MAC vulns make SANS list**

In the ongoing battle for the consumer desktop, Apple appears to be making headway to being admitted into the exclusive PC virus club.

For the first time since it's inception; SANS has listed MAC vulnerabilities in it's Top 20 list of Internet vulnerabilities. The SANS Top 20 list if published every 6 months. In the latest issue, the editors cited zero-day vulnerabilities for both the OSX operating system and the Mac Safari Web browser.
Red Herring

Related Links:
http://www.redherring.com/Article.aspx?a=16701&hed=Apple+Makes+Security+Risk+List&sector=Industries&subsector=SecurityAndDefense
http://www.businessweek.com/technology/content/may2006/tc20060504_303032.htm

- **Patch frenzy could create more problems**

CIO guest reporter Joe Basirico warns of the pitfalls created when IT departments take shortcuts to deployment and testing of patches. The article goes into detail on the possible outcomes from both mainstream and alternate patching methodologies.
CIO Update

Related Links :
http://www.cioupdate.com/trends/article.php/3601826

New Vulnerabilities Tested in SecureScout

- **16217 Ethereal IRC Protocol Dissector Denial of Service (Remote File Checking)**

Daniel Gryniewicz has reported a vulnerability in Ethereal, which potentially can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an infinite loop error in the IRC protocol dissector.

This may be exploited to cause Ethereal to go into an infinite loop, consuming all CPU resources.

The vulnerability has been reported in version 0.10.13.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00022.html

Other references:
* GENTOO:GLSA-200510-25
* URL:http://www.gentoo.org/security/en/glsa/glsa-200510-25.xml
* CONFIRM:http://www.redhat.com/archives/fedora-announce-list/2006-January/msg00005.html
* REDHAT:RHSA-2006:0156
* URL:http://www.redhat.com/support/errata/RHSA-2006-0156.html
* SGI:20060201-01-U
* URL:ftp://patches.sgi.com/support/free/security/advisories/20060201-01-U
* SUSE:SUSE-SR:2006:005
* URL:http://www.novell.com/linux/security/advisories/2006_05_sr.html
* SUSE:SUSE-SR:2005:025
* URL:http://www.novell.com/linux/security/advisories/2005_25_sr.html
* BID:15219
* URL:http://www.securityfocus.com/bid/15219
* SECTRACK:1015414
* URL:http://securitytracker.com/id?1015414
* SECUNIA:17370
* URL:http://secunia.com/advisories/17370
* SECUNIA:17377
* URL:http://secunia.com/advisories/17377
* SECUNIA:18426
* URL:http://secunia.com/advisories/18426
* SECUNIA:19130
* URL:http://secunia.com/advisories/19130
* SECUNIA:19230
* URL:http://secunia.com/advisories/19230
* SECUNIA:17480
* URL:http://secunia.com/advisories/17480
* SECUNIA:18331
* URL:http://secunia.com/advisories/18331
* SECUNIA:18911
* URL:http://secunia.com/advisories/18911

Product Homepage:
http://www.ethereal.com/

CVE Reference: CVE-2005-3313

❖ **16218 Ethereal OSPF Protocol Dissector Buffer Overflow Vulnerability (Remote File Checking)**

A vulnerability has been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially to compromise a user's system.

The vulnerability is caused due to a boundary error in the dissect_ospf_v3_address_prefix() function of the OSPF protocol dissector (packet-ospf.c) when converting received binary data to a human readable string. This can be exploited to cause a stack-based buffer overflow and may potentially allow arbitrary code execution on certain platforms.

The vulnerability has been reported in ethereal-0.10.12 RPM from Red Hat Fedora Core 3, and also in versions 0.8.20 through 0.10.13.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00022.html

Other references:
* IDEFENSE:20051209 Ethereal OSPF Protocol Dissector Buffer Overflow Vulnerability
* URL:http://www.idefense.com/application/poi/display?id=349&type=vulnerabilities
*
MISC:http://anonsvn.ethereal.com/viewcvs/viewcvs.py/trunk/epan/dissectors/packet-ospf.c
* DEBIAN:DSA-920
* URL:http://www.debian.org/security/2005/dsa-920
* GENTOO:GLSA-200512-06
* URL:http://www.gentoo.org/security/en/glsa/glsa-200512-06.xml
* REDHAT:RHSA-2006:0156
* URL:http://www.redhat.com/support/errata/RHSA-2006-0156.html
* SGI:20060201-01-U
* URL:ftp://patches.sgi.com/support/free/security/advisories/20060201-01-U
* SUSE:SUSE-SR:2006:004
* URL:http://lists.suse.de/archive/suse-security-announce/2006-Feb/0008.html
* BID:15794
* URL:http://www.securityfocus.com/bid/15794
* FRSIRT:ADV-2005-2830
* URL:http://www.frsirt.com/english/advisories/2005/2830
* SECTRACK:1015337
* URL:http://securitytracker.com/id?1015337
* SECUNIA:17973
* URL:http://secunia.com/advisories/17973
* SECUNIA:18012
* URL:http://secunia.com/advisories/18012
* SECUNIA:18062
* URL:http://secunia.com/advisories/18062
* SECUNIA:18426
* URL:http://secunia.com/advisories/18426
* SECUNIA:19230
* URL:http://secunia.com/advisories/19230
* SECUNIA:18331
* URL:http://secunia.com/advisories/18331

* SECUNIA:19012
* URL:http://secunia.com/advisories/19012
* SECUNIA:18911
* URL:http://secunia.com/advisories/18911

Product Homepage:
http://www.ethereal.com/

CVE Reference: CVE-2005-3651

❖ 16219 Ethereal GTP Dissector Denial of Service Vulnerability (Remote File Checking)

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

The vulnerability is caused due to an infinite loop error in the GTP protocol dissector. This may be exploited to cause Ethereal to go into an infinite loop, consuming all CPU resources.

The vulnerability has been reported in versions 0.9.1 through 0.10.13.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00022.html

Other references:
* REDHAT:RHSA-2006:0156
* URL:http://www.redhat.com/support/errata/RHSA-2006-0156.html
* SGI:20060201-01-U
* URL:ftp://patches.sgi.com/support/free/security/advisories/20060201-01-U
* SUSE:SUSE-SR:2006:004
* URL:http://lists.suse.de/archive/suse-security-announce/2006-Feb/0008.html
* BID:16076
* URL:http://www.securityfocus.com/bid/16076
* FRSIRT:ADV-2005-3095
* URL:http://www.frsirt.com/english/advisories/2005/3095
* OSVDB:22092
* URL:http://www.osvdb.org/22092
* SECUNIA:18229
* URL:http://secunia.com/advisories/18229
* SECTRACK:1015414
* URL:http://securitytracker.com/id?1015414
* SECUNIA:18426
* URL:http://secunia.com/advisories/18426
* SECUNIA:19230
* URL:http://secunia.com/advisories/19230
* SECUNIA:19012
* URL:http://secunia.com/advisories/19012
* SECUNIA:18911

* URL:http://secunia.com/advisories/18911

Product Homepage:
http://www.ethereal.com/

CVE Reference: CVE-2005-4585

❖ 16220 Ethereal disectors H.248, X.509if, SRVLOC , H.245, AIM, statistics counter, general packet, Crash Vulnerabilities (Remote File Checking)

Multiple unspecified vulnerabilities in Ethereal 0.10.x up to 0.10.14 allow remote attackers to cause a denial of service (crash from null dereference) via the (1) H.248, (2) X.509if, (3) SRVLOC, (4) H.245, (5) AIM, and (6) general packet dissectors; and (7) the statistics counter.

The vulnerabilities have been reported in versions 0.10.x up to 0.10.14.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00023.html

Other references:
* DEBIAN:DSA-1049
* URL:http://www.debian.org/security/2006/dsa-1049
* FEDORA:FEDORA-2006-456
* URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00194.html
* FEDORA:FEDORA-2006-461
* URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00195.html
* GENTOO:GLSA-200604-17
* URL:http://www.gentoo.org/security/en/glsa/glsa-200604-17.xml
* MANDRIVA:MDKSA-2006:077
* URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:077
* BID:17682
* URL:http://www.securityfocus.com/bid/17682
* FRSIRT:ADV-2006-1501
* URL:http://www.frsirt.com/english/advisories/2006/1501
* SECTRACK:1015985
* URL:http://securitytracker.com/id?1015985
* SECUNIA:19769
* URL:http://secunia.com/advisories/19769
* SECUNIA:19805
* URL:http://secunia.com/advisories/19805
* SECUNIA:19828
* URL:http://secunia.com/advisories/19828
* SECUNIA:19839
* URL:http://secunia.com/advisories/19839

Product Homepage:
http://www.ethereal.com/

CVE Reference: CVE-2006-1937

❖ 16221 Ethereal dissectors BER, UMA, Denial of Service Vulnerabilities (Remote File Checking)

Multiple unspecified vulnerabilities in Ethereal 0.10.x up to 0.10.14 allow remote attackers to cause a denial of service (large or infinite loops) viarafted packets to the (1) UMA and (2) BER dissectors.

The vulnerabilities have been reported in versions 0.10.x up to 0.10.14.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00023.html

Other references:
DEBIAN:DSA-1049
URL:http://www.debian.org/security/2006/dsa-1049
FEDORA:FEDORA-2006-456
URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00194.html
FEDORA:FEDORA-2006-461
URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00195.html
GENTOO:GLSA-200604-17
URL:http://www.gentoo.org/security/en/glsa/glsa-200604-17.xml
MANDRIVA:MDKSA-2006:077
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:077
BID:17682
URL:http://www.securityfocus.com/bid/17682
FRSIRT:ADV-2006-1501
URL:http://www.frsirt.com/english/advisories/2006/1501
SECTRACK:1015985
URL:http://securitytracker.com/id?1015985
SECUNIA:19769
URL:http://secunia.com/advisories/19769
SECUNIA:19805
URL:http://secunia.com/advisories/19805
SECUNIA:19828
URL:http://secunia.com/advisories/19828
SECUNIA:19839
URL:http://secunia.com/advisories/19839

Product Homepage:
http://www.ethereal.com/

CVE Reference: CVE-2006-1933

❖ 16222 Ethereal OID printing routine susceptible to an off-by-one error (Remote File Checking)

Off-by-one error in the OID printing routine in Ethereal 0.10.x up to 0.10.14 has unknown impact and remote attack vectors.

The vulnerabilities have been reported in versions 0.10.x up to 0.10.14.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00023.html

Other references:
DEBIAN:DSA-1049
URL:http://www.debian.org/security/2006/dsa-1049
FEDORA:FEDORA-2006-456
URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00194.html
FEDORA:FEDORA-2006-461
URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00195.html
GENTOO:GLSA-200604-17
URL:http://www.gentoo.org/security/en/glsa/glsa-200604-17.xml
MANDRIVA:MDKSA-2006:077
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:077
BID:17682
URL:http://www.securityfocus.com/bid/17682
FRSIRT:ADV-2006-1501
URL:http://www.frsirt.com/english/advisories/2006/1501
SECTRACK:1015985
URL:http://securitytracker.com/id?1015985
SECUNIA:19769
URL:http://secunia.com/advisories/19769
SECUNIA:19805
URL:http://secunia.com/advisories/19805
SECUNIA:19828
URL:http://secunia.com/advisories/19828
SECUNIA:19839
URL:http://secunia.com/advisories/19839

Product Homepage:
http://www.ethereal.com/

CVE Reference: CVE-2006-1932

❖ 16223 Ethereal COPS dissector, buffer overflow vulnerability (Remote File Checking)

Buffer overflow in Ethereal 0.9.15 up to 0.10.14 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via the COPS dissector.

The vulnerabilities have been reported in versions 0.9.15 up to 0.10.14

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00023.html

Other references:
DEBIAN:DSA-1049
URL:http://www.debian.org/security/2006/dsa-1049
FEDORA:FEDORA-2006-456
URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00194.html
FEDORA:FEDORA-2006-461
URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00195.html
GENTOO:GLSA-200604-17
URL:http://www.gentoo.org/security/en/glsa/glsa-200604-17.xml
MANDRIVA:MDKSA-2006:077
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:077
BID:17682
URL:http://www.securityfocus.com/bid/17682
FRSIRT:ADV-2006-1501
URL:http://www.frsirt.com/english/advisories/2006/1501
SECTRACK:1015985
URL:http://securitytracker.com/id?1015985
SECUNIA:19769
URL:http://secunia.com/advisories/19769
SECUNIA:19805
URL:http://secunia.com/advisories/19805
SECUNIA:19828
URL:http://secunia.com/advisories/19828
SECUNIA:19839
URL:http://secunia.com/advisories/19839

Product Homepage:
http://www.ethereal.com/

CVE Reference: CVE-2006-1935

❖ 16224 Ethereal ALCAP dissector, Network Instruments file code, NetXray/Windows Sniffer file code, buffer overflow vulnerabilities (Remote File Checking)

Multiple buffer overflows in Ethereal 0.10.x up to 0.10.14 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via the (1) ALCAP dissector, (2) Network Instruments file code, or (3) NetXray/Windows Sniffer file code.

The vulnerabilities have been reported in versions 0.10.x up to 0.10.14.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00023.html

Other references:
DEBIAN:DSA-1049
URL:http://www.debian.org/security/2006/dsa-1049
FEDORA:FEDORA-2006-456
URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00194.html
FEDORA:FEDORA-2006-461
URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00195.html
GENTOO:GLSA-200604-17
URL:http://www.gentoo.org/security/en/glsa/glsa-200604-17.xml
MANDRIVA:MDKSA-2006:077
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:077
BID:17682
URL:http://www.securityfocus.com/bid/17682
FRSIRT:ADV-2006-1501
URL:http://www.frsirt.com/english/advisories/2006/1501
SECTRACK:1015985
URL:http://securitytracker.com/id?1015985
SECUNIA:19769
URL:http://secunia.com/advisories/19769
SECUNIA:19805
URL:http://secunia.com/advisories/19805
SECUNIA:19828
URL:http://secunia.com/advisories/19828
SECUNIA:19839
URL:http://secunia.com/advisories/19839

Product Homepage:
http://www.ethereal.com/

CVE Reference: CVE-2006-1934

❖ 16225 Ethereal Sniffer capture, SMB PIPE dissector, Denial of Service vulnerabilities (Remote File Checking)

Multiple unspecified vulnerabilities in Ethereal 0.8.x up to 0.10.14 allow remote attackers to cause a denial of service (crash from null dereference) via the (1) Sniffer capture or (2) SMB PIPE dissector.

The vulnerabilities have been reported in versions 0.8.x up to 0.10.14.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00023.html

Other references:
DEBIAN:DSA-1049
URL:http://www.debian.org/security/2006/dsa-1049
FEDORA:FEDORA-2006-456
URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00194.html
FEDORA:FEDORA-2006-461
URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00195.html
GENTOO:GLSA-200604-17
URL:http://www.gentoo.org/security/en/glsa/glsa-200604-17.xml
MANDRIVA:MDKSA-2006:077
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:077
BID:17682
URL:http://www.securityfocus.com/bid/17682
FRSIRT:ADV-2006-1501
URL:http://www.frsirt.com/english/advisories/2006/1501
SECTRACK:1015985
URL:http://securitytracker.com/id?1015985
SECUNIA:19769
URL:http://secunia.com/advisories/19769
SECUNIA:19805
URL:http://secunia.com/advisories/19805
SECUNIA:19828
URL:http://secunia.com/advisories/19828
SECUNIA:19839
URL:http://secunia.com/advisories/19839

Product Homepage:
http://www.ethereal.com/

CVE Reference: CVE-2006-1938

❖ 16226 Ethereal invalid display filter, GSM SMS, ASN.1-based, DCERPC NT, PER, RPC, DCERPC, ASN.1 dissectors, Denial of Service vulnerabilities (Remote File Checking)

Multiple unspecified vulnerabilities in Ethereal 0.9.x up to 0.10.14 allow remote attackers to cause a denial of service (crash from null dereference) via (1) an invalid display filter, or the (2) GSM SMS, (3) ASN.1-based, (4) DCERPC NT, (5) PER, (6) RPC, (7) DCERPC, and (8) ASN.1 dissectors.

The vulnerabilities have been reported in versions 0.9.x up to 0.10.14.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00023.html

Other references:
DEBIAN:DSA-1049
URL:http://www.debian.org/security/2006/dsa-1049
FEDORA:FEDORA-2006-456
URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00194.html
FEDORA:FEDORA-2006-461
URL:http://www.redhat.com/archives/fedora-announce-list/2006-April/msg00195.html
GENTOO:GLSA-200604-17
URL:http://www.gentoo.org/security/en/glsa/glsa-200604-17.xml
MANDRIVA:MDKSA-2006:077
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:077
BID:17682
URL:http://www.securityfocus.com/bid/17682
FRSIRT:ADV-2006-1501
URL:http://www.frsirt.com/english/advisories/2006/1501
SECTRACK:1015985
URL:http://securitytracker.com/id?1015985
SECUNIA:19769
URL:http://secunia.com/advisories/19769
SECUNIA:19805
URL:http://secunia.com/advisories/19805
SECUNIA:19828
URL:http://secunia.com/advisories/19828
SECUNIA:19839
URL:http://secunia.com/advisories/19839

Product Homepage:
http://www.ethereal.com/

CVE Reference: CVE-2006-1939

New Vulnerabilities found this Week

Linux-VServer "ccaps" Insecure Capabilities Security Issue
"Escalated privileges"

Jan Rekorajski has reported a security issue in Linux-VServer, which can be exploited by malicious, local users to perform certain actions with escalated privileges.

The problem is caused by certain context capabilities, which are not limited to the guest-root. This allows users inside the guest to perform certain actions on usually restricted resources.

The security issue is reported for versions 0.09.10 to vs2.0-rc2.

References:

http://list.linux-vserver.org/archive/vserver/msg13167.html

Linux Kernel SCTP Netfilter Denial of Service Vulnerability
"Denial of Service"

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

The vulnerability is caused due to missing checks on SCTP chunk sizes in the SCTP-netfilter code and may result in an infinite loop exhausting system resources.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.13

X.Org X11 Render Extension Buffer Overflow Vulnerability
"Denial of Service; arbitrary code execution"

A vulnerability has been reported in X11, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

The vulnerability is caused due to a buffer size calculation error within the XRender extension triangle handling code. This can be exploited by a client that is authorised to connect to the X server to cause a buffer overflow.

Successful exploitation may allow arbitrary code execution.

The vulnerability has been reported in X11R6.8.x, X11R6.9.0, and X11R7.0 (xorg-server 1.0.x).

References:
http://lists.freedesktop.org/archives/xorg/2006-May/015136.html

Rsync "xattrs.diff" Patch Integer Overflow Vulnerability
"Denial of Service"

A vulnerability has been reported in rsync, which can be exploited by malicious users to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

The vulnerability is caused due to an integer overflow error in the "receive_xattr()" function within the xattrs.diff patch. This can be exploited to cause a buffer overflow and may allow arbitrary code execution via specially crafted extended attributes.

Successful exploitation requires that the "xattrs.diff" patch has been applied.

The vulnerability has been reported in version 2.6.7. Prior versions may also be affected.

References:
http://samba.anu.edu.au/ftp/rsync/rsync-2.6.8-NEWS

ClamAV Freshclam HTTP Header Buffer Overflow Vulnerability

"Denial of Service"

A vulnerability has been reported in ClamAV, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially to compromise a vulnerable system.

The vulnerability is caused due to a boundary error within the HTTP client in the Freshclam command line utility. This can be exploited to cause a stack-based buffer overflow when the HTTP headers received from a web server exceeds 8KB.

Successful exploitation requires that Freshclam is used to download virus signature updates from a malicious mirror web server e.g. via DNS poisoning.

The vulnerability has been reported in version 0.80 through 0.88.1.

References:
http://www.clamav.net/security/0.88.2.html

Linux Kernel SMBFS chroot Directory Traversal Vulnerability
"Bypass chroot restrictions"

Marcel Holtmann has reported a vulnerability in the Linux Kernel, which can be exploited by malicious, local users to bypass certain security restrictions.

The vulnerability is caused due to an input validation error in the SMBFS mounted filesystem. This can be exploited to bypass chroot restrictions via the "..\\" directory traversal sequences.

References:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=189435

Linux Kernel CIFS chroot Directory Traversal Vulnerability
"Bypass chroot restrictions"

Marcel Holtmann has reported a vulnerability in the Linux Kernel, which can be exploited by malicious, local users to bypass certain security restrictions.

The vulnerability is caused due to an input validation error in the CIFS mounted filesystem. This can be exploited to bypass chroot restrictions via the "..\\" directory traversal sequences.

The vulnerability has been reported in versions prior to 2.6.16.11.

References:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.11

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