

Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

Product Focus

[CodeRed Worm Scanner](#) – The CodeRed Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any have been infected by CodeRed Worm.

netVigilance free Single Scanners now support Windows XP Sp2. For a full list and download, go to <http://www.netvigilance.com/single scanners>

netvigilance announces support for Delta Reports in SecureScout SP.

This Week in Review

Botnets and how to protect. Cybercrime hits Japan. Kernel-level malware on the rise. Security – how to go about it.

Enjoy reading & Stay safe.

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

❖ Bots and DDoS attacks: a primer

Knowing the inner workings of botnets and their attack styles can help you formulate a defense -- or outlast an attack

My friends Paul and Robin Laudanski at CastleCops have been under a huge DDoS

attack for over a week. The attack has initiated sustained malicious loads over 1GB/s. While that number is incredible in itself, it's just on the high side of average. Some DDoS attacks come in at 10 GB/s and last for months. Many Web sites, including those dedicated to fighting spam, phishing, and malware in general, have been completely pushed off the Internet forever by DDoS attacks. The bad guys have often won.

I talked to VeriSign about the latest DNS root server attack in last week's column and mentioned that I was surprised to learn that the DNS infrastructure still isn't more inherently resistant to DDoS attacks, even after all these years and attacks. With this information and CastleCops' situation in mind, I figured that now is a good time to cover botnets and DDoS attacks.

Infoworld

Full Story :

http://www.infoworld.com/article/07/02/23/09OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/07/02/23/09OPsecadvise_1.html

❖ Japan reports 40% rise in cybercrime last year

Police report huge rise in phishing scams and spyware use.

Japan's National Police Agency (NPA) has released an annual survey of cybercrime statistics, showing a further sharp rise during 2006. Some 4,425 computer crimes were recorded by police last year, more than four times the number for 2000, when police began collating their statistics.

Among the crimes reported, password theft was thought to be a major issue, with the number of incidents involving theft of online auction site passwords more than double the previous year's figure. While scams targeting online banks showed only a slight rise, online gamers were hit by more than five times as many attacks as the previous year. Most significantly, while only 34 reports noted in 2005 involved phishing scams or the use of spyware to obtain sensitive personal data, 417 such cases were recorded in 2006.

Virusbulletin

Full Story :

http://www.virusbtn.com/news/virus_news/2007/02_23.xml?rss

❖ Kernel-level malware on the rise

Online criminals are increasingly turning to kernel-level malware to attack systems, according to security researchers at F-Secure.

Kernel-level malware acts inside the operating system's kernel, the component that links the system to the computer's hardware. Traditional malware acts like a regular application that runs on top of the operating system.

Kimmo Kasslin, a security researcher at F-Secure, said in a study that this type of malware is "a scary thought".

"It would operate with the same privileges and share all the same resources as the operating system itself, and compete with any security solutions protecting the system's integrity against any malicious activities," he wrote.

vnunet

Full Story :

<http://www.vnunet.com/vnunet/news/2184047/low-level-malware-rise-say>

❖ **Best of breed vs. big security: What's best for SMBs?**

Historically, security has been a best-of-breed market. By that, I mean customers would buy the leading product in each category and integrate the products into a cohesive whole. But now, is best of breed still the right approach? Even for small and medium-sized businesses (SMBs), which by definition are time-, resource- and money-constrained? In 1997 McAfee Inc. did a series of acquisitions, both in the networking and security space, and dubbed itself Network Associates. It was really the first security aggregator, though Axent followed that model until Symantec Corp. acquired it. The thinking was that by building a broad product line, customers would buy all the products, and growth and market domination would follow.

A decade later, we can safely say that experiment didn't work out. A few years ago, McAfee spun off pieces of the business and went back to its name and heritage. Symantec has struggled with the Axent products for years, though it keeps buying stuff and integrating it. Customers didn't want integration.

Computerweekly

Full Story :

<http://www.computerweekly.com/Articles/2007/02/19/222013/best-of-breed-vs.-big-security-whats-best-for-smbs.htm>

New Vulnerabilities Tested in SecureScout

❖ **16418 Vulnerability in Step-by-Step Interactive Training Could Allow Remote Code Execution (MS07-005/923723) (Remote File Checking)**

A remote code execution vulnerability exists in Step-by-Step Interactive Training because of the way that Step-by-Step Interactive Training handles bookmark link files. An attacker could exploit the vulnerability by constructing a specially crafted bookmark link file that could potentially allow remote code execution. An attacker

who successfully exploited this vulnerability could take complete control of an affected system. However, user interaction is required to exploit this vulnerability.

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

References:

Original advisory:

MS07-005

<http://www.microsoft.com/technet/security/Bulletin/MS07-005.msp>

Other references:

BUGTRAQ:20070213 MS Interactive Training .cbo Overflow

#

[URL:http://www.securityfocus.com/archive/1/archive/1/460009/100/0/threaded](http://www.securityfocus.com/archive/1/archive/1/460009/100/0/threaded)

CERT-VN:VU#466873

[URL:http://www.kb.cert.org/vuls/id/466873](http://www.kb.cert.org/vuls/id/466873)

BID:22484

[URL:http://www.securityfocus.com/bid/22484](http://www.securityfocus.com/bid/22484)

FRSIRT:ADV-2007-0574

[URL:http://www.frsirt.com/english/advisories/2007/0574](http://www.frsirt.com/english/advisories/2007/0574)

OSVDB:31883

[URL:http://www.osvdb.org/31883](http://www.osvdb.org/31883)

SECTrack:1017632

[URL:http://www.securitytracker.com/id?1017632](http://www.securitytracker.com/id?1017632)

SECUNIA:24121

[URL:http://secunia.com/advisories/24121](http://secunia.com/advisories/24121)

XF:ms-stepbystep-bookmark-bo(30596)

[URL:http://xforce.iss.net/xforce/xfdb/30596](http://xforce.iss.net/xforce/xfdb/30596)

CVE Reference: [CVE-2006-3448](#)

❖ 16430 Linux Kernel "do_coredump()" File Overwrite Vulnerability

A vulnerability has been reported in the Linux Kernel, which can be exploited by malicious, local users to overwrite arbitrary files.

The vulnerability is caused due to an error within the "do_coredump()" function in fs/exec.c and can be exploited to overwrite arbitrary files.

The vulnerability is reported in version 2.6.19. Other versions may also be affected.

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

References:

Original advisory:

<http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.19.1>

Other references:

TRUSTIX:2006-0074

[URL:http://www.trustix.org/errata/2006/0074/](http://www.trustix.org/errata/2006/0074/)

BID:21591

[URL:http://www.securityfocus.com/bid/21591](http://www.securityfocus.com/bid/21591)
FRSIRT:ADV-2006-5002
[URL:http://www.frsirt.com/english/advisories/2006/5002](http://www.frsirt.com/english/advisories/2006/5002)
SECUNIA:23349
[URL:http://secunia.com/advisories/23349](http://secunia.com/advisories/23349)

Product Homepage:
<http://kernel.org/>

CVE Reference: [CVE-2006-6304](#)

❖ **16431 Linux Kernel Bluetooth CAPI Messages Denial of Service**

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

The vulnerability is caused due to a boundary error within the handling of incoming CAPI messages in net/bluetooth/cmtmp/capi.c. This can be exploited to overwrite certain Kernel data structures.

The vulnerability is reported in version 2.6.19.1 Other versions may also be affected.

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

References:

Original advisory:
<http://kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.33.5>

Other references:
BUGTRAQ:20070209 rPSA-2007-0031-1 kernel

[URL:http://www.securityfocus.com/archive/1/archive/1/459615/100/0/threaded](http://www.securityfocus.com/archive/1/archive/1/459615/100/0/threaded)
MLIST:[linux-kernel] 20061215 [patch 24/24] Bluetooth: Add packet size checks for CAPI messages (CVE-2006-6106)
[URL:http://marc.theaimsgroup.com/?l=linux-kernel&m=116614741607528&w=2](http://marc.theaimsgroup.com/?l=linux-kernel&m=116614741607528&w=2)
MLIST:[linux-kernel] 20061219 Linux 2.6.18.6
[URL:http://marc.theaimsgroup.com/?l=linux-kernel&m=116648929829440&w=2](http://marc.theaimsgroup.com/?l=linux-kernel&m=116648929829440&w=2)
MISC: https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=218602
CONFIRM: <https://issues.rpath.com/browse/RPL-848>
MANDRIVA:MDKSA-2007:002
[URL:http://www.mandriva.com/security/advisories?name=MDKSA-2007:002](http://www.mandriva.com/security/advisories?name=MDKSA-2007:002)
MANDRIVA:MDKSA-2007:012
[URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:012](http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:012)
MANDRIVA:MDKSA-2007:025
[URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:025](http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:025)
REDHAT:RHSA-2007:0014
[URL:http://rhn.redhat.com/errata/RHSA-2007-0014.html](http://rhn.redhat.com/errata/RHSA-2007-0014.html)
TRUSTIX:2007-0002
[URL:http://www.trustix.org/errata/2007/0002/](http://www.trustix.org/errata/2007/0002/)
UBUNTU:USN-416-1
[URL:http://www.ubuntu.com/usn/usn-416-1](http://www.ubuntu.com/usn/usn-416-1)

BID:21604
[URL:http://www.securityfocus.com/bid/21604](http://www.securityfocus.com/bid/21604)
FRSIRT:ADV-2006-5037
[URL:http://www.frsirt.com/english/advisories/2006/5037](http://www.frsirt.com/english/advisories/2006/5037)
SECUNIA:23408
[URL:http://secunia.com/advisories/23408](http://secunia.com/advisories/23408)
SECUNIA:23427
[URL:http://secunia.com/advisories/23427](http://secunia.com/advisories/23427)
SECUNIA:23593
[URL:http://secunia.com/advisories/23593](http://secunia.com/advisories/23593)
SECUNIA:23609
[URL:http://secunia.com/advisories/23609](http://secunia.com/advisories/23609)
SECUNIA:23752
[URL:http://secunia.com/advisories/23752](http://secunia.com/advisories/23752)
SECUNIA:23997
[URL:http://secunia.com/advisories/23997](http://secunia.com/advisories/23997)
SECUNIA:24098
[URL:http://secunia.com/advisories/24098](http://secunia.com/advisories/24098)
SECUNIA:24105
[URL:http://secunia.com/advisories/24105](http://secunia.com/advisories/24105)
XF:kernel-cmtprecvinteropmsg-bo(30912)
[URL:http://xforce.iss.net/xforce/xfdb/30912](http://xforce.iss.net/xforce/xfdb/30912)

Product Homepage:
<http://kernel.org/>

CVE Reference: [CVE-2006-6106](#)

❖ **16432 Linux Kernel "mincore()", deadlock 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 exists within the handling of locking semaphores in "mincore()". This can be exploited to cause a deadlock by using the function on unmapped pages.

The vulnerability is reported in version prior to 2.6.19.2.

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

References:

Original advisory:
<http://www.kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.33.6>

Other references:
MANDRIVA:MDKSA-2007:040
[URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:040](http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:040)
REDHAT:RHSA-2007:0014
[URL:http://rhn.redhat.com/errata/RHSA-2007-0014.html](http://rhn.redhat.com/errata/RHSA-2007-0014.html)
TRUSTIX:2007-0002
[URL:http://www.trustix.org/errata/2007/0002/](http://www.trustix.org/errata/2007/0002/)
UBUNTU:USN-416-1

[URL:http://www.ubuntu.com/usn/usn-416-1](http://www.ubuntu.com/usn/usn-416-1)
BID:21663
[URL:http://www.securityfocus.com/bid/21663](http://www.securityfocus.com/bid/21663)
FRSIRT:ADV-2006-5082
[URL:http://www.frsirt.com/english/advisories/2006/5082](http://www.frsirt.com/english/advisories/2006/5082)
SECUNIA:23436
[URL:http://secunia.com/advisories/23436](http://secunia.com/advisories/23436)
SECUNIA:23609
[URL:http://secunia.com/advisories/23609](http://secunia.com/advisories/23609)
SECUNIA:23997
[URL:http://secunia.com/advisories/23997](http://secunia.com/advisories/23997)
SECUNIA:24100
[URL:http://secunia.com/advisories/24100](http://secunia.com/advisories/24100)
SECUNIA:24098
[URL:http://secunia.com/advisories/24098](http://secunia.com/advisories/24098)

Product Homepage:
<http://kernel.org/>

CVE Reference: [CVE-2006-4814](#)

❖ **16433 Linux Kernel "zlib_inflate()", memory corruption 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 exists within the "zlib_inflate()" function when processing certain data streams. This can be exploited to corrupt memory by e.g. mounting a specially crafted cramfs image and performing a read operation on the mounted file system.

The vulnerability is reported in version prior to 2.6.19.2.

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

References:

Original advisory:
<http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.19.2>

Other references:
MISC: <http://projects.info-pull.com/mokb/MOKB-07-11-2006.html>
REDHAT:RHSA-2007:0014
[URL:http://rhn.redhat.com/errata/RHSA-2007-0014.html](http://rhn.redhat.com/errata/RHSA-2007-0014.html)
SUSE:SUSE-SA:2006:079
[URL:http://www.novell.com/linux/security/advisories/2006_79_kernel.html](http://www.novell.com/linux/security/advisories/2006_79_kernel.html)
UBUNTU:USN-416-1
[URL:http://www.ubuntu.com/usn/usn-416-1](http://www.ubuntu.com/usn/usn-416-1)
SECUNIA:22767
[URL:http://secunia.com/advisories/22767](http://secunia.com/advisories/22767)
SECUNIA:23997
[URL:http://secunia.com/advisories/23997](http://secunia.com/advisories/23997)
SECUNIA:24098
[URL:http://secunia.com/advisories/24098](http://secunia.com/advisories/24098)

Product Homepage:

<http://kernel.org/>

CVE Reference: [CVE-2006-5823](#)

❖ **16434 Linux Kernel Ext2 file system, failures to handle corrupted data structures Vulnerability**

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

The Kernel fails to handle corrupted data structures in the Ext2 file system correctly. This can be exploited to crash the system by mounting and reading a specially crafted file system image.

The vulnerability is reported in version prior to 2.6.19.2.

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

References:

Original advisory:

<http://projects.info-pull.com/mokb/MOKB-12-11-2006.html>

Other references:

<http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.19.2>

Product Homepage:

<http://kernel.org/>

CVE Reference:

❖ **16435 Linux Kernel "listxattr" Memory Corruption 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) or potentially gain escalated privileges.

The vulnerability is caused due to an error within the "listxattr" system call when interpreting "bad_inode_ops" return values, which can be exploited to cause a memory corruption.

Successful exploitation requires a bad inode.

The vulnerability is reported in version prior to 2.6.20.

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

References:

Original advisory:

<http://lkml.org/lkml/2007/1/3/150>

Other references:

MANDRIVA:MDKSA-2007:040

[URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:040](http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:040)

REDHAT:RHSA-2007:0014

[URL:http://www.redhat.com/support/errata/RHSA-2007-0014.html](http://www.redhat.com/support/errata/RHSA-2007-0014.html)

UBUNTU:USN-416-1

[URL:http://www.ubuntu.com/usn/usn-416-1](http://www.ubuntu.com/usn/usn-416-1)

BID:22316

[URL:http://www.securityfocus.com/bid/22316](http://www.securityfocus.com/bid/22316)

SECUNIA:23955

[URL:http://secunia.com/advisories/23955](http://secunia.com/advisories/23955)

SECUNIA:23997

[URL:http://secunia.com/advisories/23997](http://secunia.com/advisories/23997)

SECUNIA:24100

[URL:http://secunia.com/advisories/24100](http://secunia.com/advisories/24100)

SECUNIA:24098

[URL:http://secunia.com/advisories/24098](http://secunia.com/advisories/24098)

Product Homepage:

<http://kernel.org/>

CVE Reference: [CVE-2006-5753](#)

❖ **16436 Linux Kernel "key_alloc_serial()" Denial of Service**

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

The vulnerability is caused due to a NULL pointer dereference within the "key_alloc_serial()" function, which can be exploited to crash the Kernel.

The vulnerability is reported in version prior to 2.6.20.1

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

References:

Original advisory:

http://bugzilla.kernel.org/show_bug.cgi?id=7727

https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=227495

Other references:

BID:22539

[URL:http://www.securityfocus.com/bid/22539](http://www.securityfocus.com/bid/22539)

SECUNIA:24109

[URL:http://secunia.com/advisories/24109](http://secunia.com/advisories/24109)

Product Homepage:

<http://kernel.org/>

CVE Reference: [CVE-2007-0006](#)

❖ 16438 Mozilla Firefox "locations.hostname" DOM Property Handling Vulnerability (Remote File Checking)

Michal Zalewski has reported a vulnerability in Mozilla Firefox, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to an error in the handling of the "locations.hostname" DOM property. This can be exploited to e.g. manipulate authentication cookies for an arbitrary web site via assigning a URL including a NULL character ("\x00") to "locations.hostname".

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

The vulnerability is reported in version 2.0.0.1. Other versions may also be affected.

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

References:

Original Advisories:

https://bugzilla.mozilla.org/show_bug.cgi?id=370445

Other references:

FULLDISC:20070215 Firefox: serious cookie stealing / same-domain bypass vulnerability

[URL:http://www.securityfocus.com/archive/1/460217/100/0/threaded](http://www.securityfocus.com/archive/1/460217/100/0/threaded)

FULLDISC:20070215 Re: [Full-disclosure] Firefox: serious cookie stealing / same-domain bypass vulnerability

[URL:http://www.securityfocus.com/archive/1/460217/100/0/threaded](http://www.securityfocus.com/archive/1/460217/100/0/threaded)

MISC: <http://lcamtuf.dione.cc/ffhostname.html>

CERT-VN:VU#885753

[URL:http://www.kb.cert.org/vuls/id/885753](http://www.kb.cert.org/vuls/id/885753)

BID:22566

[URL:http://www.securityfocus.com/bid/22566](http://www.securityfocus.com/bid/22566)

FRSIRT:ADV-2007-0624

[URL:http://www.frsirt.com/english/advisories/2007/0624](http://www.frsirt.com/english/advisories/2007/0624)

SECTrack:1017654

[URL:http://securitytracker.com/id?1017654](http://securitytracker.com/id?1017654)

SECUNIA:24175

[URL:http://secunia.com/advisories/24175](http://secunia.com/advisories/24175)

XF:firefox-locationhostname-security-bypass(32533)

[URL:http://xforce.iss.net/xforce/xfdb/32533](http://xforce.iss.net/xforce/xfdb/32533)

Product HomePage:

<http://www.mozilla.org/products/firefox/>

CVE Reference: [CVE-2007-0981](https://cve.mitre.org/cve/2007/0981)

❖ 16439 Mozilla Firefox "_blank" Phishing Weakness (Remote File Checking)

Michal Zalewski has discovered a weakness in Firefox, which can be exploited by malicious people to conduct phishing attacks.

The weakness is caused due to Firefox allowing scripts to open a tab with a blank address bar and add arbitrary content to it. This can further be exploited to spoof the user interface, including setting the title to an arbitrary value.

The weakness is confirmed in version 2.0.0.1. Other versions may also be affected.

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

References:

Original Advisories:

20070216 Firefox: about:blank is phisher's best friend

<http://www.securityfocus.com/archive/1/archive/1/460369/100/0/threaded>

Other references:

BUGTRAQ:20070217 Re: Firefox: about:blank is phisher's best friend

#

[URL:http://www.securityfocus.com/archive/1/archive/1/460412/100/0/threaded](http://www.securityfocus.com/archive/1/archive/1/460412/100/0/threaded)

BID:22601

[URL:http://www.securityfocus.com/bid/22601](http://www.securityfocus.com/bid/22601)

Product HomePage:

<http://www.mozilla.org/products/firefox/>

CVE Reference: [CVE-2007-1004](#)

New Vulnerabilities found this Week

PHP-Nuke HTTP "referer" SQL Injection Vulnerability

"SQL injection attacks"

Maciej "krasza" Kukla has discovered a vulnerability in PHP-Nuke, which can be exploited by malicious people to conduct SQL injection attacks.

Input passed via the "referer" HTTP header in index.php is not properly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

The vulnerability is confirmed in version 7.9 and reported in version 8.0. Other versions may also be affected.

References:

<http://secunia.com/advisories/24224/>

Cisco Unified IP Conference Station / IP Phone Default Accounts

"Bypass the user authentication; Access device; Denial of Service; Gain escalated privileges"

Some security issues have been reported in Cisco Unified IP Conference Station and IP Phones, which can be exploited by malicious people to access a vulnerable device.

1) A design error in way the administrative HTTP interface of Cisco Unified IP Conference Station handles the state of administrator login sessions can be exploited to bypass the user authentication by accessing management URLs directly.

2) A hard-coded user account on various Cisco Unified IP Phones can be exploited to remotely access the CLI (Command Line Interface) of a vulnerable IP phone. This can further be exploited to cause a DoS (Denial of Service) or gain escalated privileges.

References:

<http://www.cisco.com/warp/public/707/cisco-sa-20070221-phone.shtml>

<http://www.cisco.com/warp/public/707/cisco-air-20070221-phone.shtml>

Nortel Net Direct Client for Linux Privilege Escalation

“Gain escalated privileges”

Jon Hart has reported a vulnerability in Net Direct Client for Linux, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused by a combination of insecure permissions and a race condition when downloading and executing client binaries. This can be exploited to execute arbitrary commands with root privileges when a user uses the VPN client.

The vulnerability is reported in versions 6.0.1 through 6.0.3.

References:

<http://www130.nortelnetworks.com/go/main.jsp?cscat=BLTNDETAIL&DocumentOID=540071>

http://spoofed.org/blog/archive/2007/02/nortel_vpn_unix_client_local_root_compromise.html

Linux Kernel NFSACL "ACCESS" Denial of Service

“Denial of Service”

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

The vulnerability is caused due to an invalid freeing of a pointer when handling NFSACL 2 "ACCESS" requests, which can be exploited to crash the kernel.

References:

<http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.20.1>

Snort DCE/RPC Preprocessor Buffer Overflow

“Execution of arbitrary code”

eel Mehta has reported a vulnerability in Snort, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error within the DCE/RPC preprocessor when reassembling SMB Write AndX requests. This can be exploited to cause a stack-based buffer overflow via a specially crafted packet sent over a network that is monitored by Snort.

Successful exploitation allows execution of arbitrary code.

The vulnerability reportedly affects the following versions:

- * Snort 2.6.1, 2.6.1.1, and 2.6.1.2

- * Snort 2.7.0 beta 1

References:

<http://www.iss.net/threats/257.html>

<http://www.snort.org/docs/advisory-2007-02-19.html>

<http://www.kb.cert.org/vuls/id/196240>

Mac OS X Security Update Fixes Multiple Vulnerabilities

“Execution of arbitrary code; Application crash”

Apple has issued a security update for Mac OS X, which fixes multiple vulnerabilities.

1) A boundary error exists in Finder, which can be exploited by malicious people to cause a buffer overflow by tricking a user to mount a malicious disk image.

Successful exploitation may allow execution of arbitrary code.

2) A null-pointer dereference error in iChat Bonjour can be exploited by malicious people to cause the application to crash.

NOTE: A similar issue exists in Mac OS X 10.3.

3) A format string error in the handling of AIM URLs in iChat can be exploited by malicious people to possibly execute arbitrary code.

Successful exploitation requires that a user is tricked into accessing a specially crafted AIM URL.

4) An error in the UserNotificationCenter can be exploited by malicious, local users to gain escalated privileges.

References:

<http://docs.info.apple.com/article.html?artnum=305102>

Mozilla Firefox "_blank" Phishing Weakness

“Phishing attacks”

Michal Zalewski has discovered a weakness in Firefox, which can be exploited by malicious people to conduct phishing attacks.

The weakness is caused due to Firefox allowing scripts to open a tab with a blank address bar and add arbitrary content to it. This can further be exploited to spoof the user interface, including setting the title to an arbitrary value.

The weakness is confirmed in version 2.0.0.1. Other versions may also be affected.

References:

<http://archives.neohapsis.com/archives/bugtraq/2007-02/0324.html>

SpamAssassin Long URI Denial of Service

“Denial of Service”

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

The vulnerability is caused due to an unspecified error and can be exploited to cause a DoS via overly long URIs in the message content.

References:

<http://svn.apache.org/repos/asf/spamassassin/branches/3.1/build/announcements/3.1.8.txt>

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@seurescout.net