ScoutNews
The weekly Security update from the makers of SecureScout
December 26, 2008

2008 Issue #52

Table of Contents

Product Focus

Task Scheduler Vulnerability Scanner - The S4 Task Scheduler Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Task Scheduler flaw (MS04-022).

Download Here:
http://www.netvigilance.com/productdownloads?productname=taskschedulervulnerabilityscanner

This Week in Review

Beware when you decide on layoffs. Argument: High usability equals low security. Nokia sells profitable security business. A look at security when funds are tight.

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

- **Security Manager\'s Journal: Massive layoff is a security issue**

December 22, 2008 (Computerworld) It's been a rough week. Today, my company announced a 15% cut in its workforce, or about 1,000 employees.

My first task was to identify any layoff candidates who represented single points of failure, meaning they were the only employees who could perform a particular critical job function. Single points of failure, human or otherwise, are a bad idea. But it happens, and it's better to recognize them in advance than to realize your mistake after they've left the company.

Trouble Ticket Issue: A 15% reduction in the company's workforce means access to systems must be secured appropriately.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=331151&source=rss_topic17

- **Small laptops pose a big security threat**

December 22, 2008 (Computerworld) They're highly portable, inexpensive, very popular -- and a potential security nightmare. Running against the trend of mobile computers featuring progressively larger processors, memory, storage, screens and price tags, ultraportable laptops promise to streamline and simplify their users' lives. Easy to carry, capable of running only a handful of modest applications and affordably priced, ultraportables have emerged over the past year or so to become one of the hottest mobile computing trends.

"It's a technology with great appeal to many people," observes Gabriel Vitus, IT director at the Certified General Accountants' Association of Canada, a trade organization in Vancouver, British Columbia.

"This is a threat that IT managers are just beginning to recognize," says Brian Wolfe, a security analyst at Lazarus Technologies Inc., an IT consulting service in Itasca, Ill.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=330656&source=rss_topic17

- **Nokia offloads security business to Check Point**

December 23, 2008 (Techworld.com) Nokia has finally found a buyer for its profitable security appliance business. From the first quarter of 2009, the division will belong to partner Check Point, the companies have announced.

The sell-off is not a surprise, even if Check Point's interest hardened late in the day. Nokia's line of remote access and firewall security hardware was built around the Israeli company's software at its core and is considered to have a good reputation. The deal gives Check Point much needed market share.

"This business fits naturally with Check Point, and the combination will provide a great path forward for the thousands of customers who depend on Nokia security solutions today."

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9124280&source=rss_topic1

- **What can you afford NOT to do on IT security?**

December 22, 2008 (Computerworld) With the ailing economy putting a crimp in IT budgets, information security managers -- like just about everyone else in the tech world -- are feeling pressure to keep their costs in line.

"It's imperative to squeeze every penny of value out of everything you do," said Jim Kirby, senior network engineer at DataWare Services, an IT services firm in Sioux Falls, S.D. This is a good time to stop working on "marginal" projects and redirect resources to security capabilities that are absolutely necessary, Kirby said.

And Fenwick & West is taking some steps to cut costs. The firm is deferring an earlier plan to hire a full-time networking and security expert because of the recession, Kesner said. It is also looking for opportunities to use open-source alternatives to some of its security tools.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=331453&source=rss_topic17

New Vulnerabilities Tested in SecureScout

- **18217 Oracle Application Server - Oracle Reports Developer component unspecified Vulnerability (oct-2008/CVE-2008-2619)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Oracle Reports Developer" component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html

* FRSIRT: ADV-2008-2825
http://www.frsirt.com/english/advisories/2008/2825
* SECTRACK: 1021054
http://www.securitytracker.com/id?1021054
* SECTRACK: 1021057
http://www.securitytracker.com/id?1021057
* SECUNIA: 32291
http://secunia.com/advisories/32291

CVE Reference:

CVE-2008-2619 (cve.mitre.org, nvd.nist.gov)

• 18218 Oracle Application Server - Oracle JDeveloper component unspecified Vulnerability (oct-2008/CVE-2008-2588)

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Oracle JDeveloper" component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html
* FRSIRT: ADV-2008-2825
http://www.frsirt.com/english/advisories/2008/2825
* SECTRACK: 1021054
http://www.securitytracker.com/id?1021054
* SECUNIA: 32291
http://secunia.com/advisories/32291
* XF: oracle-jdeveloper-info-disclosure(45877)
http://xforce.iss.net/xforce/xfdb/45877

CVE Reference:

CVE-2008-2588 (cve.mitre.org, nvd.nist.gov)

• 18219 Oracle Application Server - Oracle Discoverer Administrator component unspecified Vulnerability (oct-2008/CVE-2008-3986)

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Oracle Discoverer Administrator" component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html
* FRSIRT: ADV-2008-2825
http://www.frsirt.com/english/advisories/2008/2825
* SECTRACK: 1021054
http://www.securitytracker.com/id?1021054
* SECUNIA: 32291
http://secunia.com/advisories/32291
* XF: oracle-appserver-discadmin-info-disclosure(45889)
http://xforce.iss.net/xforce/xfdb/45889

CVE Reference:

CVE-2008-3986 (cve.mitre.org, nvd.nist.gov)

• 18220 Oracle Application Server - Oracle Discoverer Desktop component unspecified Vulnerability (oct-2008/CVE-2008-3987)

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Oracle Discoverer Desktop" component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html
* FRSIRT: ADV-2008-2825

http://www.frsirt.com/english/advisories/2008/2825
* SECTRACK: 1021054
http://www.securitytracker.com/id?1021054
* SECUNIA: 32291
http://secunia.com/advisories/32291
* XF: oracle-appserver-discdesk-info-disclosure(45890)
http://xforce.iss.net/xforce/xfdb/45890

CVE Reference:

CVE-2008-3987 (cve.mitre.org, nvd.nist.gov)

- **18221 Malformed SNMP Message-Handling Vulnerabilities (cisco-sa-20020212-snmp-msgs)**

Cisco products contain multiple vulnerabilities in handling of SNMP requests and traps. A general report for multiple vendors was initially published on February 12 (Bugtraq IDs 4088 and 4089), however more information is now available and a separate Bugtraq ID has been allocated for the Cisco IOS vulnerabilities.
It is reportedly possible for a remote attacker to create a denial of service by transmitting malformed SNMP packet to a device running a vulnerable version of IOS. The affected device may reset, or (under rare circumstances) require a manual reset to regain functionality.
The nature of these denial of service conditions is not known. They may be due to exploitable buffer overflow conditions.

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

References:

* MISC:
http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/snmpv1/index.html
* CERT: CA-2002-03
http://www.cert.org/advisories/CA-2002-03.html
* ISS: 20020212 PROTOS Remote SNMP Attack Tool
http://www.iss.net/security_center/alerts/advise110.php
* CERT-VN: VU#107186
http://www.kb.cert.org/vuls/id/107186
* REDHAT: RHSA-2001:163
http://www.redhat.com/support/errata/RHSA-2001-163.html
* CALDERA: CSSA-2002-SCO.4
http://lists.virus.org/bugtraq-0202/msg00168.html
* HP: HPSBMP0206-015
http://www.securityfocus.com/advisories/4211
* SGI: 20020201-01-A
ftp://patches.sgi.com/support/free/security/advisories/20020201-01-A
* MS: MS02-006
http://www.microsoft.com/technet/security/bulletin/MS02-006.asp
* BID: 5043
http://www.securityfocus.com/bid/5043
* OVAL: oval:org.mitre.oval:def:144
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:144
* OVAL: oval:org.mitre.oval:def:161
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:161
* OVAL: oval:org.mitre.oval:def:298
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:298
* OVAL: oval:org.mitre.oval:def:1048
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1048
* CERT-VN: VU#854306
http://www.kb.cert.org/vuls/id/854306
* SUNALERT: 57404
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57404-1
* OVAL: oval:org.mitre.oval:def:87
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:87
* MISC:
http://www.sans.org/top20/2003/#U7
* CISCO: cisco-sa-20020212-snmp-msgs
http://www.cisco.com/warp/public/707/cisco-sa-20020212-snmp-msgs.shtml

CVE Reference:

CVE-2002-0013 (cve.mitre.org, nvd.nist.gov)
CVE-2002-0012 (cve.mitre.org, nvd.nist.gov)

• 18222 Cisco IOS Software SNMP Read-Write ILMI Community String Vulnerability (cisco-sa-20010227-ios-snmp-ilmi)

Cisco IOS Software releases based on versions 11.x and 12.0 contain a defect that allows a limited number of SNMP objects to be viewed and modified without authorization using a undocumented ILMI community string. Some of the modifiable objects are confined to the MIB-II system group, such as "sysContact", "sysLocation", and "sysName", that do not affect the device's normal operation but that may cause confusion if modified unexpectedly. The remaining objects are contained in the LAN-EMULATION-CLIENT and PNNI MIBs, and modification of those objects may affect ATM configuration. An affected device might be vulnerable to a denial-of-service attack if it is not protected against unauthorized use of the ILMI community string.

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

References:

* CISCO: 20010207 Cisco IOS Software SNMP Read-Write ILMI Community String Vulnerability
http://www.cisco.com/warp/public/707/ios-snmp-ilmi-vuln-pub.shtml
* XF: cisco-ios-modify-snmp(6169)
http://xforce.iss.net/xforce/xfdb/6169

CVE Reference:

CVE-2001-0711 (cve.mitre.org, nvd.nist.gov)

• 18223 Apache mod_negotiation CRLF injection Vulnerability

CRLF injection vulnerability in the mod_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary HTTP headers and conduct HTTP response splitting attacks by uploading a file with a multi-line name containing HTTP header sequences and a file extension, which leads to injection within a "406 Not Acceptable" or "300 Multiple Choices" HTTP response when the extension is omitted in a request for the file.

The issue is fixed in versions 1.3.40, 2.0.62, and 2.2.7.

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

References:

* BUGTRAQ: 20080122 Apache mod_negotiation Xss and Http Response Splitting
http://www.securityfocus.com/archive/1/archive/1/486847/100/0/threaded
* MISC:
http://www.mindedsecurity.com/MSA01150108.html
* GENTOO: GLSA-200803-19
http://security.gentoo.org/glsa/glsa-200803-19.xml
* BID: 27409
http://www.securityfocus.com/bid/27409
* SECTRACK: 1019256
http://securitytracker.com/id?1019256
* SECUNIA: 29348
http://secunia.com/advisories/29348
* SREASON: 3575
http://securityreason.com/securityalert/3575
* XF: apache-modnegotiation-response-splitting(39893)
http://xforce.iss.net/xforce/xfdb/39893

CVE Reference:

CVE-2008-0456 (cve.mitre.org, nvd.nist.gov)

• 18224 Apache mod_negotiation Cross-site scripting (XSS) Vulnerability

Cross-site scripting (XSS) vulnerability in the mod_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary web script or HTML by uploading a file with a name containing XSS sequences and a file extension, which leads to injection within a "406 Not Acceptable" or "300 Multiple Choices" HTTP response when the extension is omitted in a request for the file.

The issue is fixed in versions 1.3.40, 2.0.62, and 2.2.7.

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

References:

* BUGTRAQ: 20080122 Apache mod_negotiation Xss and Http Response Splitting
http://www.securityfocus.com/archive/1/archive/1/486847/100/0/threaded
* MISC:
http://www.mindedsecurity.com/MSA01150108.html
* GENTOO: GLSA-200803-19
http://security.gentoo.org/glsa/glsa-200803-19.xml
* BID: 27409
http://www.securityfocus.com/bid/27409
* SECTRACK: 1019256
http://securitytracker.com/id?1019256
* SECUNIA: 29348
http://secunia.com/advisories/29348
* SREASON: 3575
http://securityreason.com/securityalert/3575
* XF: apache-modnegotiation-xss(39867)
http://xforce.iss.net/xforce/xfdb/39867

CVE Reference:

CVE-2008-0455 (cve.mitre.org, nvd.nist.gov)

• 18225 Apache mod_ssl access control Vulnerability

mod_ssl in Apache 2.0 up to 2.0.55, and 2.2 up to 2.2.1 when configured with an SSL vhost with access control and a custom error 400 error page, allows remote attackers to cause a denial of service (application crash) via a non-SSL request to an SSL port, which triggers a NULL pointer dereference.

The issue is fixed in versions 2.0.58, and 2.2.2.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Crash** Risk: **Medium**

References:

* MISC:
http://svn.apache.org/viewcvs?rev=358026&view=rev
* CONFIRM:
http://issues.apache.org/bugzilla/show_bug.cgi?id=37791
* CONFIRM:
http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd?mode=18&ID=3117
* CONFIRM:
http://support.avaya.com/elmodocs2/security/ASA-2006-250.htm
* APPLE: APPLE-SA-2008-05-28
http://lists.apple.com/archives/security-announce/2008//May/msg00001.html
* FEDORA: FEDORA-2006-052
http://www.redhat.com/archives/fedora-announce-list/2006-January/msg00060.html
* FEDORA: FLSA-2006:175406
http://www.securityfocus.com/archive/1/archive/1/425399/100/0/threaded
* GENTOO: GLSA-200602-03
http://www.gentoo.org/security/en/glsa/glsa-200602-03.xml
* HP: HPSBUX02145
http://www.securityfocus.com/archive/1/archive/1/445206/100/0/threaded
* HP: HPSBUX02172
http://www.securityfocus.com/archive/1/archive/1/450315/100/0/threaded
* HP: HPSBMA02328
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01428449
* REDHAT: RHSA-2006:0159
http://rhn.redhat.com/errata/RHSA-2006-0159.html
* SGI: 20060101-01-U
ftp://patches.sgi.com/support/free/security/advisories/20060101-01-U
* SUNALERT: 102640
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102640-1
* SUNALERT: 102662
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102662-1
* SUSE: SuSE-SA:2006:051
http://lists.suse.com/archive/suse-security-announce/2006-Sep/0004.html
* SUSE: SUSE-SA:2006:051
http://www.novell.com/linux/security/advisories/2006_51_apache.html
* TRUSTIX: TSLSA-2005-0074
http://www.trustix.org/errata/2005/0074/
* UBUNTU: USN-241-1
http://www.ubuntulinux.org/usn/usn-241-1

* CERT: TA08-150A
http://www.us-cert.gov/cas/techalerts/TA08-150A.html
* BID: 16152
http://www.securityfocus.com/bid/16152
* FRSIRT: ADV-2006-0056
http://www.frsirt.com/english/advisories/2006/0056
* FRSIRT: ADV-2006-3920
http://www.frsirt.com/english/advisories/2006/3920
* FRSIRT: ADV-2006-3995
http://www.frsirt.com/english/advisories/2006/3995
* FRSIRT: ADV-2006-4207
http://www.frsirt.com/english/advisories/2006/4207
* FRSIRT: ADV-2006-4300
http://www.frsirt.com/english/advisories/2006/4300
* FRSIRT: ADV-2006-4868
http://www.frsirt.com/english/advisories/2006/4868
* FRSIRT: ADV-2008-1246
http://www.frsirt.com/english/advisories/2008/1246/references
* FRSIRT: ADV-2008-1697
http://www.frsirt.com/english/advisories/2008/1697
* SECTRACK: 1015447
http://securitytracker.com/id?1015447
* SECUNIA: 18307
http://secunia.com/advisories/18307
* SECUNIA: 18340
http://secunia.com/advisories/18340
* SECUNIA: 18333
http://secunia.com/advisories/18333
* SECUNIA: 18339
http://secunia.com/advisories/18339
* SECUNIA: 18429
http://secunia.com/advisories/18429
* SECUNIA: 18585
http://secunia.com/advisories/18585
* SECUNIA: 18517
http://secunia.com/advisories/18517
* SECUNIA: 18743
http://secunia.com/advisories/18743
* SECUNIA: 19012
http://secunia.com/advisories/19012
* SECUNIA: 21848
http://secunia.com/advisories/21848
* SECUNIA: 22233
http://secunia.com/advisories/22233
* SECUNIA: 22368
http://secunia.com/advisories/22368
* SECUNIA: 22523
http://secunia.com/advisories/22523
* SECUNIA: 22669
http://secunia.com/advisories/22669
* SECUNIA: 23260
http://secunia.com/advisories/23260
* SECUNIA: 22992
http://secunia.com/advisories/22992
* SECUNIA: 29849
http://secunia.com/advisories/29849
* SECUNIA: 30430
http://secunia.com/advisories/30430

CVE Reference:

CVE-2005-3357 (cve.mitre.org, nvd.nist.gov)

• 18237 Excel File Format Parsing Vulnerability (CVE-2008-4265) (MS08-074/959070) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Office Excel as a result of memory corruption when loading Excel records. The vulnerability could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed object. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

* MS: MS08-074
http://www.microsoft.com/technet/security/Bulletin/MS08-074.mspx
* FRSIRT: Microsoft Office Excel Multiple Code Execution Vulnerabilities (MS08-074)
http://www.vupen.com/english/Reference-CVE-2008-4266.php
* SECUNIA: 31593
http://secunia.com/advisories/31593/
* SECTRACK: 1021368
http://securitytracker.com/alerts/2008/Dec/1021368.html
* BID: 32618
http://www.securityfocus.com/bid/32618

CVE Reference:

CVE-2008-4265 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-5557 PHP CVSS 2.0 Score = 10.0

Heap-based buffer overflow in ext/mbstring/libmbfl/filters/mbfilter_htmlent.c in the mbstring extension in PHP 4.3.0 through 5.2.6 allows context-dependent attackers to execute arbitrary code via a crafted string containing an HTML entity, which is not properly handled during Unicode conversion, related to the (1) mb_convert_encoding, (2) mb_check_encoding, (3) mb_convert_variables, and (4) mb_parse_str functions.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

XF: http://xforce.iss.net/xforce/xfdb/47525

BID: http://www.securityfocus.com/bid/32948

CONFIRM: http://www.php.net/ChangeLog-5.php#5.2.7

SECTRACK: http://securitytracker.com/id?1021482

CONFIRM: http://cvs.php.net/viewvc.cgi/php-src/ext/mbstring/libmbfl/filters/mbfilter_htmlent.c?r1=1.7&r2=1.8

CONFIRM: http://bugs.php.net/bug.php?id=45722

FULLDISC: http://archives.neohapsis.com/archives/fulldisclosure/2008-12/0477.html

CVE Reference: CVE-2008-5557

• CVE-2008-5702 Linux CVSS 2.0 Score = 7.2

Buffer underflow in the ibwdt_ioctl function in drivers/watchdog/ib700wdt.c in the Linux kernel before 2.6.28-rc1 might allow local users to have an unknown impact via a certain /dev/watchdog WDIOC_SETTIMEOUT IOCTL call.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

CONFIRM: http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.28-rc1

MLIST: http://openwall.com/lists/oss-security/2008/12/17/9

MLIST: http://openwall.com/lists/oss-security/2008/12/17/6

MLIST: http://openwall.com/lists/oss-security/2008/12/17/20

MLIST: http://openwall.com/lists/oss-security/2008/12/10/2

MLIST: http://lkml.org/lkml/2008/10/5/173

CONFIRM:

http://git.kernel.org/?p=linux/kernel/git/stable/linux-2.6.27.y.git;a=commit;h=7c2500f17d65092d93345f3996cf82ebca17e9ff

CONFIRM: http://bugzilla.kernel.org/show_bug.cgi?id=11399

CVE Reference: CVE-2008-5702

- **CVE-2008-5715 Mozilla CVSS 2.0 Score = 5.0**

Mozilla Firefox 3.0.5 on Windows Vista allows remote attackers to cause a denial of service (application crash) via JavaScript code with a long string value for the hash property (aka location.hash).

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

BID: http://www.securityfocus.com/bid/32988

MILW0RM: http://www.milw0rm.com/exploits/7554

CVE Reference: CVE-2008-5715

- **CVE-2008-5713 Linux CVSS 2.0 Score = 4.9**

The __qdisc_run function in net/sched/sch_generic.c in the Linux kernel before 2.6.25 on SMP machines allows local users to cause a denial of service (soft lockup) by sending a large amount of network traffic, as demonstrated by multiple simultaneous invocations of the Netperf benchmark application in UDP_STREAM mode.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=477744

BID: http://www.securityfocus.com/bid/32985

MLIST: http://openwall.com/lists/oss-security/2008/12/23/1

CONFIRM: http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.25

CONFIRM: http://git.kernel.org/?p=linux/kernel/git/stable/linux-2.6.27.y.git;a=commit;h=2ba2506ca7ca62c56edaa334b0fe61eb5eab6a

CVE Reference: CVE-2008-5713

- **CVE-2008-5701 Linux CVSS 2.0 Score = 4.7**

Array index error in arch/mips/kernel/scall64-o32.S in the Linux kernel before 2.6.28-rc8 on 64-bit MIPS platforms allows local users to cause a denial of service (system crash) via an o32 syscall with a small syscall number, which leads to an attempted read operation outside the bounds of the syscall table.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

CONFIRM: http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.28-rc8

MLIST: http://openwall.com/lists/oss-security/2008/12/09/1

CONFIRM: http://git.kernel.org/?p=linux/kernel/git/stable/linux-2.6.27.y.git;a=commit;h=e807f9574e37a3f202e677feaaad1b7c5d2c0db

CVE Reference: CVE-2008-5701

- **CVE-2008-5699 Sun CVSS 2.0 Score = 4.6**

The name service cache daemon (nscd) in Sun Solaris 10 and OpenSolaris snv_50 through snv_104 does not properly check permissions, which allows local users to gain privileges and obtain sensitive information via unspecified vectors.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

BID: http://www.securityfocus.com/bid/32921

SUNALERT: http://sunsolve.sun.com/search/document.do?assetkey=1-26-242006-1

SECTRACK: http://securitytracker.com/id?1021477

CVE Reference: CVE-2008-5699

- **CVE-2008-5700 Linux CVSS 2.0 Score = 4.6**

libata in the Linux kernel before 2.6.27.9 does not set minimum timeouts for SG_IO requests, which allows local users to cause a denial of service (Programmed I/O mode on drives) via multiple simultaneous invocations of an unspecified test program.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=474495

CONFIRM: http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.27.9

MLIST: http://openwall.com/lists/oss-security/2008/12/09/2

CONFIRM: http://git.kernel.org/?p=linux/kernel/git/stable/linux-2.6.27.y.git;a=commit;h=f2f1fa78a155524b849edf359e42a3001ea652c

CVE Reference: CVE-2008-5700

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