netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 5

February 2, 2007

Table of Contents

Product Focus

Task Scheduler Vulnerability Scanner – The 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).

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

netvigilance announces support for Delta Reports in SecureScout SP.

This Week in Review

Online Fraud Survey shows user concern. Which applications do actually have the most vulnerabilities? MicroSoft to offer new vulnerability detection process to application developers. Background on 'Storm' Worm.

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

- **Findings of RSA's Annual Financial Institution Online Fraud Survey**

RSA, The security division of EMC, today released the findings of its fourth annual Financial Institution Consumer Online Fraud Survey. Conducted in December 2006,

the online survey asked 1,678 adults from eight countries around the world for their opinions on evolving fraud threats such as phishing, vishing and keylogging, and on the efforts of their financial institutions to strengthen remote channel banking authentication.

Key results of the survey include:

* 91% of account-holders answered that they are willing to start using a new authentication method, beyond the standard 'username-and-password', if their banks decided to offer stronger security

* 73% commented that they would like their financial institution to use risk-based authentication

* 69% of account-holders believe that financial institutions should replace username-and-password log-in with stronger authentication for online banking

* 58% of account-holders believe that financial institutions should deploy stronger authentication for telephone banking

HardwareZone

Full Story :
http://www.hardwarezone.com/news/view.php?id=6524&cid=5

❖ Vulnerability counts do matter

It happened again! I got into yet another argument...er...heated discussion over the security of Microsoft Windows versus some other operating system. Usually it starts with some reader's knee-jerk emotional reaction -- saying "Windows sucks!" or something like that.
When faced with a knee-jerker (aka "jerk"), I often point out that it's easy for any OS to be insecure if the admin doesn't follow best practices, but it's just as simple for me to secure almost most any OS if I follow basic security practices.

Normally, my critics counter that remark by saying that because Windows has so many more vulnerabilities than the average competing OS, it's easier to secure those other OSes. Unless you're running OpenBSD, this statement is usually untrue. All of those other OSes end up with a fair amount of published vulnerabilities that need to be patched.

These days it's easy for me to point to vulnerability counts as a metric of Microsoft's better job at security. (My favorite site for vulnerability statistics is Secunia.com, and their Software Inspector scanner is a good source.) For instance, IIS 5 had 14 announced holes. IIS 6, released almost four years ago in March 2003, has had three known holes, none popularly exploited. Apache Web server, IIS's nearest competitor, has had more than 33 vulnerabilities in the same time period.

InfoWorld

Full Story :
http://www.infoworld.com/article/07/02/02/06OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/07/02/02/06OPsecadvise_1.html

- **Microsoft, Symantec Might Clash in Application Security**

With malware code writers creating an increasing number of attacks aimed at exploiting vulnerabilities in software applications, in addition to their threats that target operating system flaws, longtime partners Symantec and Microsoft are both attempting to stake major claims in the application security market.
While Symantec's play is more straightforward, having targeted the sector with a range of products and services since 2005, Microsoft is believed to be readying a slew of offerings it will market to third-party software developers to help those firms drum potential vulnerabilities out of their products.

Microsoft's failure to identify weak points in its own software, specifically its Windows OS, has been a highly publicized issue for many years, but the company claims to have turned over a new leaf.

In the process of building its newly launched Windows Vista OS, the Redmond, Wash.-based software maker employed a new vulnerability detection process labeled SDL (Security Development Lifecycle), that claims to have greatly reduced the number of holes in its products, and which will also serve as a foundation for the firm's nascent applications security business.

ExtremeTech

Full Story :
http://www.extremetech.com/article2/0,1697,2089711,00.asp

- **Worm bypasses gatekeepers**

The Storm Worm continues to evade traditional anti-virus software, says US-based Commtouch.

A report released by the company says the worm makes use of four offensive manoeuvres that virtually guarantee it will "continue evading traditional anti-virus".

The document, "Malware Outbreak Trend Report: Storm Worm", details the characteristics of the Storm Worm, a server-side polymorphic malware.

Its four key tactics include its high-distribution intensity, variety of variants, the limited life of these variants, and the fact that each variety is distributed in relatively small quantities or instances.

ITWeb

Full Story :
http://www.itweb.co.za/sections/software/2007/0702021400.asp?A=SEC&S=Security&T=Section&O=FPSH

New Vulnerabilities Tested in SecureScout

- **16402 NetBackup bpcd daemon, arbitrary code execution via long**

request with a malformed length prefix (Remote File Checking)

This vulnerability allows attackers to execute arbitrary code on vulnerable installations of Symantec Veritas NetBackup. Authentication is not required to exploit this vulnerability.

The specific flaw exists within bpcd.exe during the parsing of overly long requests to a NetBackup Master/Media Server. Communications to this process are prefixed with a length, which, if malformed can result in a stack based buffer overflow. Exploitation of this vulnerability can lead to complete system compromise.

The following versions are vulnerable to the issue:
Symantec Veritas NetBackup 5.0 before 5.0_MP7, 5.1 before 5.1_MP6, and 6.0 before 6.0_MP4

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

References:

Original advisory:
http://www.zerodayinitiative.com/advisories/ZDI-06-049.html
http://www.symantec.com/avcenter/security/Content/2006.12.13a.html

Other references:
BUGTRAQ:20061213 ZDI-06-049: Symantec Veritas NetBackup Long Request Buffer Overflow Vulnerability
#
URL:http://www.securityfocus.com/archive/1/archive/1/454313/100/0/threaded
CERT-VN:VU#607312
URL:http://www.kb.cert.org/vuls/id/607312
BID:21565
URL:http://www.securityfocus.com/bid/21565
FRSIRT:ADV-2006-4999
URL:http://www.frsirt.com/english/advisories/2006/4999
SECTRACK:1017379
URL:http://securitytracker.com/id?1017379
SECUNIA:23368
URL:http://secunia.com/advisories/23368
XF:netbackup-long-request-bo(30882)
URL:http://xforce.iss.net/xforce/xfdb/30882
XF:netbackup-connect-options-bo(30883)
URL:http://xforce.iss.net/xforce/xfdb/30883

Product homepage:
http://www.symantec.com/enterprise/products/overview.jsp?pcid=1018&pvid=2_1

CVE Reference: CVE-2006-6222

❖ **16403 NetBackup bpcd daemon, arbitrary code execution via a long CONNECT_OPTIONS request (Remote File Checking)**

This vulnerability allows attackers to execute arbitrary code on vulnerable installations

of Symantec Veritas NetBackup. Authentication is not required to exploit this vulnerability.

The specific flaw exists within bpcd.exe during the parsing of overly long CONNECT_OPTIONS requests to a NetBackup Master/Media Server. When the CONNECT_OPTIONS command is parsed, the contents are copied into a stack allocated buffer without proper length checking. Exploitation of this vulnerability can lead to complete system compromise.

The following versions are vulnerable to the issue:
Symantec Veritas NetBackup 5.0 before 5.0_MP7, 5.1 before 5.1_MP6, and 6.0 before 6.0_MP4

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

References:

Original advisory:
http://www.zerodayinitiative.com/advisories/ZDI-06-050.html
http://www.symantec.com/avcenter/security/Content/2006.12.13a.html

Other references:
BUGTRAQ:20061213 ZDI-06-050: Symantec Veritas NetBackup CONNECT_OPTIONS Buffer Overflow Vulnerability
#
URL:http://www.securityfocus.com/archive/1/archive/1/454314/100/0/threaded
CERT-VN:VU#650432
URL:http://www.kb.cert.org/vuls/id/650432
BID:21565
URL:http://www.securityfocus.com/bid/21565
FRSIRT:ADV-2006-4999
URL:http://www.frsirt.com/english/advisories/2006/4999
SECTRACK:1017379
URL:http://securitytracker.com/id?1017379
SECUNIA:23368
URL:http://secunia.com/advisories/23368
XF:netbackup-connect-options-bo(30883)
URL:http://xforce.iss.net/xforce/xfdb/30883

Product homepage:
http://www.symantec.com/enterprise/products/overview.jsp?pcid=1018&pvid=2_1

CVE Reference: CVE-2006-5822

❖ 16404 NetBackup bpcd daemon, arbitrary code execution via malicious chained commands (Remote File Checking)

This vulnerability allows attackers to execute arbitrary code on vulnerable installations of Symantec Veritas NetBackup. Authentication is not required to exploit this vulnerability.

The NetBackup bpcd daemon (bpcd.exe) in Symantec Veritas NetBackup 5.0 before 5.0_MP7, 5.1 before 5.1_MP6, and 6.0 before 6.0_MP4 does not properly check for chained commands, which allows remote attackers to execute arbitrary commands by appending malicious commands to valid commands.

The following versions are vulnerable to the issue:
Symantec Veritas NetBackup 5.0 before 5.0_MP7, 5.1 before 5.1_MP6, and 6.0 before 6.0_MP4

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

References:

Original advisory:
http://www.symantec.com/avcenter/security/Content/2006.12.13a.html

Other references:
ISS:20061213 Symantec Veritas Netbackup 5.0/5.1 and 6.0 Logic Vulnerability
URL:http://www.iss.net/threats/247.html
CERT-VN:VU#252936
URL:http://www.kb.cert.org/vuls/id/252936
BID:21565
URL:http://www.securityfocus.com/bid/21565
FRSIRT:ADV-2006-4999
URL:http://www.frsirt.com/english/advisories/2006/4999
SECTRACK:1017379
URL:http://securitytracker.com/id?1017379
SECUNIA:23368
URL:http://secunia.com/advisories/23368
XF:backup-invalid-input(27638)

Product homepage:
http://www.symantec.com/enterprise/products/overview.jsp?pcid=1018&pvid=2_1

CVE Reference: CVE-2006-4902

❖ 16405 NetBackup Sharepoint Services server daemon (bpspsserver), arbitrary code execution via crafted Request Service packets to the vnetd service (Remote File Checking)

This vulnerability allows remote attackers to execute arbitrary code on vulnerable Symantec VERITAS NetBackup client and server installations.

This specific flaw exists within specially crafted messages to the vnetd service, listening on TCP port 13724 via opcode 6 (Request Service). An attacker can overrun two fixed size buffers, one on the stack, and the other in the .data section of the executable.

In the main function of bpspsserver, a call to get_adaptable_string() at 0x0040243A reads in a variable length string from the network in the form of '[len][string]'. This string is then copied via a sprintf() at 0x00402458, and a swprintf() at 0x00402479 into two different fixed sized buffers. The first buffer is on the stack and the second buffer is a

global variable.

The following versions are vulnerable to the issue:
Symantec Veritas NetBackup 6.0 before 6.0_MP2

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

References:

Original advisory:
http://www.tippingpoint.com/security/advisories/TSRT-06-01.html
http://securityresponse.symantec.com/avcenter/security/Content/2006.03.27.html
http://seer.support.veritas.com/docs/281521.htm

Other references:
BUGTRAQ:20060327 TSRT-06-01: Symantec VERITAS NetBackup vnetd Buffer Overflow Vulnerability
URL:http://www.securityfocus.com/archive/1/archive/1/428979/100/0/threaded
CERT-VN:VU#377441
URL:http://www.kb.cert.org/vuls/id/377441
BID:17264
URL:http://www.securityfocus.com/bid/17264
FRSIRT:ADV-2006-1124
URL:http://www.frsirt.com/english/advisories/2006/1124
SECTRACK:1015832
URL:http://securitytracker.com/id?1015832
SECUNIA:19417
URL:http://secunia.com/advisories/19417
XF:netbackup-vnetd-bo(25473)
URL:http://xforce.iss.net/xforce/xfdb/25473

Product homepage:
http://www.symantec.com/enterprise/products/overview.jsp?pcid=1018&pvid=2_1

CVE Reference: CVE-2006-0991

❖ 16406 NetBackup Catalog daemon (bpdbm), arbitrary code execution via unknown vectors (Remote File Checking)

This vulnerability allows remote attackers to execute arbitrary code on vulnerable Symantec VERITAS NetBackup installations. Authentication is not required to exploit this vulnerability.

The specific flaw exists within the NetBackup Database Manager service (bpdbm.exe) due to insufficient bounds checking during a call to sprintf() that copies user-supplied data to a stack-based buffer. The vulnerable daemon listens on TCP port 13721.

The following versions are vulnerable to the issue:
Symantec Veritas NetBackup 5.0 before 5.0_MP6_S01/5.0_MP7, 5.1 before 5.1_MP4_S01/5.1_MP5, and 6.0 before 6.0_MP2

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

References:

Original advisory:
http://www.zerodayinitiative.com/advisories/ZDI-06-006.html
http://securityresponse.symantec.com/avcenter/security/Content/2006.03.27.html
http://seer.support.veritas.com/docs/281521.htm

Other references:
BUGTRAQ:20060327 SYM06-006, Veritas NetBackup: Multiple Overflow Vulnerabilities in NetBackup Daemons
URL:http://www.securityfocus.com/archive/1/archive/1/428992/100/0/threaded
BUGTRAQ:20060327 ZDI-06-006: Symantec VERITAS NetBackup Database Manager Buffer Overflow
URL:http://www.securityfocus.com/archive/1/archive/1/428988/100/0/threaded
CERT-VN:VU#744137
URL:http://www.kb.cert.org/vuls/id/744137
BID:17264
URL:http://www.securityfocus.com/bid/17264
FRSIRT:ADV-2006-1124
URL:http://www.frsirt.com/english/advisories/2006/1124
SECTRACK:1015832
URL:http://securitytracker.com/id?1015832
SECUNIA:19417
URL:http://secunia.com/advisories/19417
XF:netbackup-bpdbm-sprintf-bo(25472)
URL:http://xforce.iss.net/xforce/xfdb/25472

Product homepage:
http://www.symantec.com/enterprise/products/overview.jsp?pcid=1018&pvid=2_1

CVE Reference: CVE-2006-0990

❖ 16407 NetBackup volume manager daemon (vmd), arbitrary code execution via unknown vectors (Remote File Checking)

This vulnerability allows remote attackers to execute arbitrary code on vulnerable Symantec VERITAS NetBackup installations. Authentication is not required to exploit this vulnerability.

This specific flaw exists within the volume manager daemon (vmd.exe) due to incorrect bounds checking during a call to sscanf() that copies user-supplied data to a stack-based buffer. The vulnerable daemon listens on TCP port 13701.

The following versions are vulnerable to the issue:
Symantec Veritas NetBackup 5.0 before 5.0_MP6_S01/5.0_MP7, 5.1 before 5.1_MP4_S01/5.1_MP5, and 6.0 before 6.0_MP2

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

References:

Original advisory:
http://www.zerodayinitiative.com/advisories/ZDI-06-005.html
http://securityresponse.symantec.com/avcenter/security/Content/2006.03.27.html
http://seer.support.veritas.com/docs/281521.htm

Other references:
BUGTRAQ:20060327 ZDI-06-005: Symantec VERITAS NetBackup Volume Manager Buffer Overflow
URL:http://www.securityfocus.com/archive/1/archive/1/428944/100/0/threaded
CERT-VN:VU#880801
URL:http://www.kb.cert.org/vuls/id/880801
BID:17264
URL:http://www.securityfocus.com/bid/17264
FRSIRT:ADV-2006-1124
URL:http://www.frsirt.com/english/advisories/2006/1124
OSVDB:24172
URL:http://www.osvdb.org/24172
SECTRACK:1015832
URL:http://securitytracker.com/id?1015832
XF:netbackup-vmd-sscanf-bo(25471)
URL:http://xforce.iss.net/xforce/xfdb/25471

Product homepage:
http://www.symantec.com/enterprise/products/overview.jsp?pcid=1018&pvid=2_1

CVE Reference: CVE-2006-0989

❖ 16408 NetBackup volume manager daemon (vmd), arbitrary code execution via a crafted packet (Remote File Checking)

iDefense Labs notified Symantec of a buffer overflow vulnerability in VERITAS NetBackup that could potentially allow a remote attacker to cause a denial of service or to execute arbitrary code. The vulnerability was initially found in the NetBackup vmd but further analysis revealed the problem occurs in a shared library used by vmd possibly impacting other daemons using that shared library also. The buffer overflow condition is due to improper bounds checking of user input. If a remote attacker were able to gain access to the affected library through one of the daemons and successfully exploit this vulnerability, they could potentially disrupt backup capabilities or possibly execute arbitrary code with elevated privileges on the targeted system.

The following versions are vulnerable to the issue:
Symantec Veritas NetBackup 5.0 before NB_50_5S2_M, 5.1 before NB_51_3AS2_M

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

References:

Original advisory:
20051110 Stack Overflow in Veritas Netbackup Enterprise Server
http://www.idefense.com/application/poi/display?id=336&type=vulnerabilities
http://seer.support.veritas.com/docs/279553.htm

http://securityresponse.symantec.com/avcenter/security/Content/2005.11.08b.html

Other references:
BUGTRAQ:20060115 Veritas NetBackup "Volume Manager Daemon" Module Stack Overflow - Exploit
URL:http://www.securityfocus.com/archive/1/422066/100/0/threaded
BUGTRAQ:20060117 Re: Veritas NetBackup "Volume Manager Daemon" Module Stack Overflow - Exploit
URL:http://www.securityfocus.com/archive/1/422157/100/0/threaded
CERT-VN:VU#574662
URL:http://www.kb.cert.org/vuls/id/574662
BID:15353
URL:http://www.securityfocus.com/bid/15353
FRSIRT:ADV-2005-2349
URL:http://www.frsirt.com/english/advisories/2005/2349
OSVDB:20674
URL:http://www.osvdb.org/20674
SECTRACK:1015170
URL:http://securitytracker.com/id?1015170
SECUNIA:17503
URL:http://secunia.com/advisories/17503
XF:netbackup-vmd-bo(22985)
URL:http://xforce.iss.net/xforce/xfdb/22985

Product homepage:
http://www.symantec.com/enterprise/products/overview.jsp?pcid=1018&pvid=2_1

CVE Reference: CVE-2005-3116

❖ 16409 NetBackup Java user interface service (bpjava-msvc) daemon, arbitrary code execution via the COMMAND_LOGON_TO_MSERVER command (Remote File Checking)

This vulnerability allows remote attackers to execute arbitrary code on vulnerable NetBackup installations. Authentication is not required to exploit this vulnerability.

This specific flaw exists within the bpjava-msvc daemon due to incorrect handling of format string data passed through the 'COMMAND_LOGON_TO_MSERVER' command. The vulnerable daemon listens on TCP port 13722 and affects both NetBackup clients and servers.

The following versions are vulnerable to the issue:
Symantec Veritas NetBackup 5.0 before NB_50_5S1320_M, 5.1 before NB_51_3AS0949_M, 6.0 before NB_60_3S0007_M

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

References:

Original advisory:
http://www.zerodayinitiative.com/advisories/ZDI-05-001.html
http://www.symantec.com/avcenter/security/Content/2005.10.12.html

http://seer.support.veritas.com/docs/279085.htm

Other references:
VULNWATCH:20051012 ZDI-05-001: VERITAS NetBackup Remote CodeExecution
SUNALERT:102054
URL:http://sunsolve.sun.com/search/document.do?assetkey=1-26-102054-1
CERT-VN:VU#495556
URL:http://www.kb.cert.org/vuls/id/495556
BID:15079
URL:http://www.securityfocus.com/bid/15079
SECTRACK:1015028
URL:http://securitytracker.com/id?1015028
SECUNIA:17181
URL:http://secunia.com/advisories/17181

Product homepage:
http://www.symantec.com/enterprise/products/overview.jsp?pcid=1018&pvid=2_1

CVE Reference: CVE-2005-2715

❖ 16410 NetBackup NDMP server, remote denial of service attacks (Remote File Checking)

Hat-Squad has reported a weakness in NetBackup, which can be exploited by malicious people to cause a DoS (Denial of Service).

The problem is caused due to a NULL pointer dereference error in the NDMP mover agent and can be exploited via a specially crafted NDMP CONFIG message to crash the current listening child process spawned when the connection attempt was made.

The following versions are vulnerable to the issue:
Symantec Veritas NetBackup 5.1 before NB_51_3AS0949_M

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

References:

Original advisory:
http://www.hat-squad.com/en/000170.html

Other references:
SECUNIA:16187
http://secunia.com/advisories/16187

Product homepage:
http://www.symantec.com/enterprise/products/overview.jsp?pcid=1018&pvid=2_1

CVE Reference: CVE-2005-2389

❖ 16411 NetBackup Administrative Assistant interface, arbitrary commands execution via the bpjava-susvc process (Remote File Checking)

When the NetBackup Administrative Java GUI connects to a NetBackup server (either a master or media server) a process is started on the server called bpjava-susvc. A normal user with access to this server could send specially crafted commands to this process and have those commands executed with root authority.

It is also possible to exploit this issue if the Backup & Restore GUI is started as root.

The following versions are vulnerable to the issue:
Symantec Veritas NetBackup 5.0 before 5.0MP4, 5.1 before 5.1MP2

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

References:

Original advisory:
http://seer.support.veritas.com/docs/271727.htm

Other references:
CERT-VN:VU#685456
URL:http://www.kb.cert.org/vuls/id/685456
CIAC:P-020
URL:http://www.ciac.org/ciac/bulletins/p-020.shtml
BID:11494
URL:http://www.securityfocus.com/bid/11494
SECUNIA:12901
URL:http://secunia.com/advisories/12901/
XF:nebackup-bpjavasusvc-gain-privileges(17811)
URL:http://xforce.iss.net/xforce/xfdb/17811

Product homepage:
http://www.symantec.com/enterprise/products/overview.jsp?pcid=1018&pvid=2_1

CVE Reference: CVE-2004-1389

New Vulnerabilities found this Week

Microsoft Word Unspecified String Handling Memory Corruption
"Execution of arbitrary code"

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

The vulnerability is caused due to an unspecified error when parsing strings in Word documents and can be exploited to corrupt memory thereby allowing execution of arbitrary code on the user's system.

NOTE: The vulnerability is currently being actively exploited.

The vulnerability is reported in Microsoft Word 2000. Other versions may also be affected.

References:

http://www.microsoft.com/technet/security/advisory/932114.mspx
http://blogs.technet.com/msrc/archive/2007/01/26/microsoft-security-advisory-932114-posted.aspx
http://www.kb.cert.org/vuls/id/412225

Wireshark Multiple Denial of Service Vulnerabilities

"Denial of Service"

Some vulnerabilities have been reported in Wireshark, which can be exploited by malicious people to cause a DoS (Denial of Service).

Errors within the TCP, HTTP, IEEE 802.11, and LLT parsers can be exploited to cause a crash or consume large amounts of memory when parsing a specially crafted packet that is either captured off the wire or loaded via a capture file.

The vulnerabilities are reported in various versions prior to 0.99.5.

References:
http://www.wireshark.org/security/wnpa-sec-2007-01.html

Sun Solaris ICMP Denial of Service Vulnerability

"Denial of Service"

Sun has acknowledged a vulnerability in Solaris, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error when processing ICMP ping requests and can be exploited to cause a system panic by sending a specially crafted ICMP request to an affected system.

Successful exploitation requires that systems are configured to receive ICMP ping requests.

The vulnerability is reported in Sun Solaris 10 for both the SPARC and x86 platform.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102697-1
http://www.kb.cert.org/vuls/id/967236

Cisco IOS SIP Packet Handling Reload Denial of Service

"Denial of Service"

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

The vulnerability is caused due to an error when handling certain SIP packets and can be exploited to cause the device to reload via a specially crafted packet sent to port 5060.

Successful exploitation requires that the device supports voice and is not configured for SIP.

Please see the vendor's advisory for a list of affected products and versions.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml
http://www.cisco.com/warp/public/707/cisco-air-20070131-sip.shtml
http://www.kb.cert.org/vuls/id/438176

Linux Kernel "listxattr" Memory Corruption Vulnerability

"Denial of Service; gain escalated privileges"

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.

References:
http://lkml.org/lkml/2007/1/3/150

Yahoo Messenger Contact Details Script Execution Vulnerability

"Arbitrary script code execution"

Hai Nam Luke has discovered a vulnerability in Yahoo Messenger, which potentially can be exploited by malicious users to compromise a user's system.

Input passed to the "First Name", "Last Name", and "Nickname" fields in the "Contact Details" option is not properly sanitized when displaying status notification messages to the user in a chat box. This can e.g. be exploited to execute a limited amount of arbitrary script code in the Local Zone (My Computer) context by inputting specially crafted image tags in the aforementioned fields, tricking a target user into adding the attacker to the messenger list, sending a message to the target user, and then changing the status e.g. from "Available" to "Invisible To Everyone".

Successful exploitation requires that the attacker is in the messenger list of the target.

NOTE: When a user adds another user to the messenger list, the contact details get truncated, which limits the amount of script code that can be inserted.

The vulnerability is confirmed in version 8.1.0.209. Other versions may also be affected.

References:
http://archives.neohapsis.com/archives/bugtraq/2007-01/0613.html

Cisco IOS VTP Denial of Service Vulnerability

"Denial of Service"

David Barroso Berrueta and Alfredo Andres Omella have reported a vulnerability in Cisco

IOS, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error when handling certain malformed VLAN Trunking Protocol (VTP) packets. This can be exploited to cause a device to reload by sending a specially crafted VTP packet.

Successful exploitation requires knowledge of the VTP domain name and the port that is configured for trunking.

The vulnerability is reported in the following devices:
* Cisco 2900XL Series Switches
* Cisco 2950 Series Switches
* Cisco 2955 Series Switches
* Cisco 3500XL Series Switches
* Cisco 3550 Series Switches
* Cisco 3570 Series Switches

References:
http://www.cisco.com/en/US/products/products_security_response09186a00807d1a81.html
http://www.s21sec.com/es/avisos/s21sec-034-en.txt

Sun Solaris FreeType Integer Overflow and Underflow Vulnerabilities
"Denial of Service"

Sun has acknowledged some vulnerabilities in Solaris, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise applications using the library.

The vulnerabilities affect Solaris 8, 9, and 10 on the SPARC and x86 platform.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102705-1
http://secunia.com/advisories/20100/

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