netVigilance

ScoutNews Team

January 20, 2006
2006 Issue # 3

Weekly ScoutNews by netVigilance

Table of Contents

SecureScout NX gets Major Overhaul.

The NX Update this week contains more than 40 major bugfixes and improvements, which affect more than 1500 test cases. The Protocol ID has been improved to ensure better execution speed, drastic improvement (up to 130%) are seen in environments with many secure servers, https imaps, smtps etc.

Upgrades are free to all current SecureScout Subscribers in good standing.

This Week in Review

DoD gets hacked, Symantec patches 'feature', desktop security tips, FBI to open Cyber-Security Center in Louisiana and Windows WiFi an open door.

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

- **Spanish youth cracks into DoD computer**

An 18 year old Spanish youth was charged by the Spanish Civil Guard for breaking into US Department of Defense systems at the Point Loma submarine base in San Diego. The charge carries serious implications since the perpetrator is now an adult. Sources claim that 'fun' was the motivation.

Full Story:
http://www.securitypronews.com/insiderreports/insider/spn-49-20060116SpanishHackerCrackedDefenseDepartment.html

❖ Symantec patches flaw caused by SystemWorks spyware

The discovery a hidden directory called NProtect that was designed to prevent users from accidentally deleting important files by Mark Russinovich of the Finnish company F-Secure; not only set off the Spyware alarm but raised the concern for virus' to creep in since the secret directory is not scanned by AV.

RedHerring

Full Story :
http://www.redherring.com/Article.aspx?a=15306&hed=Norton+Security+Flaw+Patched

❖ Tips on securing the data on your desktop

Good tips from PC Pro staff on protecting a desktop from intrusion. All of the basics are covered, firealling, AV, encryption and strong passwords. The article also contains some sage advice on how to use all of these tools in concert.

PCPro

Full Story :

http://www.pcpro.co.uk/security/features/33928/lock-down-your-pc.html

❖ FBI to open cyber crime center

The FBI announced the opening of a cybercrime center to be located in Baton Rouge, LA to investigate crimes perpetrated by cyber-crooks such as identity thieves, child pornographers, hackers and fraud operators.

Cybercrime is the FBIs third-highest priority ranking just behind anti-terrorism and foreign counterintelligence and ranking above public corruption. Special Agent James Bernazzani, in charge of the FBIs New Orleans office was quoted saying "The criminal element in all facets is moving into the cyberworld, the terrorists use it, fraud guys use it, violent criminals use it, drug cartels use it, street gangs use it. We've got to be ahead of the curve."

Associated Press

Full Story :
http://www.nola.com/newsflash/louisiana/index.ssf?/base/news-22/1137420847252900.xml&storylist=louisiana

- ### Windows XP, 2000 wireless vulnerability

A “feature” in Windows XP and 2000 WiFi utilities can create an opportunity for hackers to gain access to unsuspecting wireless laptop users.

Mark Loveless, an expert on computer security; claims that hackers could gain access via a peer-to-peer connection that is created when Windows searches for and fails to find a wireless access point (WAP). When the Windows laptop fails to find a WAP, the machine will then broadcast this SSID, looking for other nearbycomputers to connect to.
TMCnet

Related Links :
http://news.tmcnet.com/news/it/-windows-wi-fi-vulnerability-discovered-/2006/jan/1290932.htm

New Vulnerabilities Tested in SecureScout

- ### 16088 Linux Kernel IA32 Compatibility "execve()" Buffer Overflow Vulnerability

Ilja van Sprundel has reported a vulnerability 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 a race condition in the compatibility code for "execve()" on the IA64 and AMD64 platforms that occurs when counting and copying arguments from user-space to kernel-space.

Successful exploitation crashes the kernel and may allow execution of arbitrary code with escalated privileges.

The vulnerability has been reported in versions 2.4.31 and prior, and in versions 2.6.6 and prior.

The vulnerability has been fixed in version 2.4.32-pre1 and 2.6.7.

Test Case Impact: **Gather Info** Vulnerability Impact: **Denial of Service** Risk: **Medium**

References:

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.32.log
http://www.suresec.org/advisories/adv4.pdf

Other references:
http://secunia.com/advisories/15980/

Product HomePage:
http://kernel.org/

CVE Reference: CAN-2005-1768

❖ 16089 Linux Kernel error exists in the handling of access to ar.rsc via ptrace and restore_sigcontext Vulnerability

A vulnerability has been reported in the Linux kernel. It can be exploited by malicious, local users to cause a DoS (Denial of Service), or by malicious people to bypass certain security restrictions.

An error exists in the handling of access to ar.rsc via ptrace and restore_sigcontext.

The vulnerability has been fixed in version 2.6.12.1.

Test Case Impact: **Gather Info** Vulnerability Impact: **Denial of Service** Risk: **Medium**

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.1
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12
http://www.kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.32.log

Other references:
http://secunia.com/advisories/15786/

Product HomePage:
http://kernel.org/

CVE Reference:
CAN-2005-1761
CAN-2005-1762
CAN-2005-1763
CAN-2005-1767
CAN-2005-1913
CAN-2005-3108
CAN-2005-3109
CVE-2005-3272

❖ 16090 Linux Kernel error in the delivery of signals to cause kernel panic Vulnerability

A vulnerability has been reported in the Linux kernel. It can be exploited by malicious, local users to cause a DoS (Denial of Service), or by malicious people to bypass certain security restrictions.

An error in the delivery of signals can cause a kernel panic when a sub-thread "exec" with a pending timer.

The vulnerability has been fixed in version 2.6.12.1.

Test Case Impact: **Gather Info** Vulnerability Impact: **Denial of Service** Risk: **Medium**

References:
Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.1
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12
http://www.kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.32.log

Other references:
http://secunia.com/advisories/15786/

Product HomePage:
http://kernel.org/

CVE Reference:
CAN-2005-1761
CAN-2005-1762
CAN-2005-1763
CAN-2005-1767
CAN-2005-1913
CAN-2005-3108
CAN-2005-3109
CVE-2005-3272

❖ 16091 Linux Kernel error in "ptrace()" when processing specially crafted addresses to cause kernel crash Vulnerability

A vulnerability has been reported in the Linux kernel. It can be exploited by malicious, local users to cause a DoS (Denial of Service), or by malicious people to bypass certain security restrictions.

An error in "ptrace()" when processing specially crafted addresses on the AMD64 platform can cause the kernel to crash.

The vulnerability has been fixed in version 2.6.12.1.

Test Case Impact: **Gather Info** Vulnerability Impact: **Denial of Service** Risk: **Medium**

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.1
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12
http://www.kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.32.log

Other references:
http://secunia.com/advisories/15786/

Product HomePage:
http://kernel.org/

CVE Reference:
CAN-2005-1761
CAN-2005-1762
CAN-2005-1763
CAN-2005-1767
CAN-2005-1913
CAN-2005-3108
CAN-2005-3109
CVE-2005-3272

❖ 16092 Linux Kernel error in the stack segment fault handler in "/arch/x86_64/kernel/traps.c" may be exploited to crash the kernel Vulnerability

A vulnerability has been reported in the Linux kernel. It can be exploited by malicious, local users to cause a DoS (Denial of Service), or by malicious people to bypass certain security restrictions.

An error in the stack segment fault handler in "/arch/x86_64/kernel/traps.c" may be exploited to crash the kernel via a stack fault exception.

The vulnerability has been fixed in version 2.6.12.1 and 2.4.32-pre1.

Test Case Impact: **Gather Info** Vulnerability Impact: **Denial of Service** Risk: **Medium**

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.1
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12
http://www.kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.32.log

Other references:
http://secunia.com/advisories/15786/

Product HomePage:
http://kernel.org/

CVE Reference:
CAN-2005-1761
CAN-2005-1762
CAN-2005-1763
CAN-2005-1767
CAN-2005-1913
CAN-2005-3108
CAN-2005-3109
CVE-2005-3272

❖ 16093 Linux Kernel error in "/x86_64/kernel/ptrace.c" to crash the kernel Vulnerability

A vulnerability has been reported in the Linux kernel. It can be exploited by malicious, local users to cause a DoS (Denial of Service), or by malicious people to bypass certain security restrictions.

An off-by one quadword error in "/x86_64/kernel/ptrace.c" can potentially be exploited to crash the kernel by writing a word 40 bytes into the page above the kernel stack of a process.

The vulnerability has been fixed in version 2.6.12.1.

Test Case Impact: **Gather Info** Vulnerability Impact: **Denial of Service** Risk: **Medium**

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.1
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12
http://www.kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.32.log

Other references:
http://secunia.com/advisories/15786/

Product HomePage:
http://kernel.org/

CVE Reference:
CAN-2005-1761
CAN-2005-1762
CAN-2005-1763
CAN-2005-1767
CAN-2005-1913
CAN-2005-3108
CAN-2005-3109
CVE-2005-3272

❖ 16094 Linux Kernel error in "mm/ioremap.c" may be exploited by local users to cause a denial of service or to disclose certain information Vulnerability

A vulnerability has been reported in the Linux kernel. It can be exploited by malicious, local users to cause a DoS (Denial of Service), or by malicious people to bypass certain security restrictions.

An error in "mm/ioremap.c" on the x86_64 platform may be exploited by local users to cause a denial of service or to disclose certain information by performing an "iremap" on certain memory maps that causes a lookup of a page that does not exist.

The vulnerability has been fixed in version 2.6.12.1.

Test Case Impact: **Gather Info** Vulnerability Impact: **Denial of Service** Risk: **xxxxxxxx**

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.1
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12
http://www.kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.32.log

Other references:
http://secunia.com/advisories/15786/

Product HomePage:
http://kernel.org/

CVE Reference:
CAN-2005-1761
CAN-2005-1762
CAN-2005-1763
CAN-2005-1767
CAN-2005-1913
CAN-2005-3108
CAN-2005-3109
CVE-2005-3272

❖ 16095 Linux Kernel HFS and HFS+ file system drivers to crash the kernel Vulnerability

A vulnerability has been reported in the Linux kernel. It can be exploited by malicious, local users to cause a DoS (Denial of Service), or by malicious people to bypass certain security restrictions.

The HFS and HFS+ file system drivers do not properly verify that the file system to be mounted is really HFS/HFS+. This may be exploited by users who can mount file systems to crash the kernel by using hfsplus to mount a filesystem that is not hfsplus.

The vulnerability has been fixed in version 2.6.12.1.

Test Case Impact: **Gather Info** Vulnerability Impact: **Denial of Service** Risk: **Medium**

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.1
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12
http://www.kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.32.log

Other references:
http://secunia.com/advisories/15786/

Product HomePage:
http://kernel.org/

CVE Reference:
CAN-2005-1761
CAN-2005-1762
CAN-2005-1763
CAN-2005-1767
CAN-2005-1913
CAN-2005-3108
CAN-2005-3109
CVE-2005-3272

❖ 16096 Linux Kernel bridge to forward packets with spoofed source addresses Vulnerability

A vulnerability has been reported in the Linux kernel. It can be exploited by malicious, local users to cause a DoS (Denial of Service), or by malicious people to bypass certain security restrictions.

It is possible to poison the bridge forwarding table by frames that have been dropped by filtering. This may be exploited to cause the bridge to forward packets with spoofed source addresses.

The vulnerability has been fixed in version 2.6.12.1.

Test Case Impact: **Gather Info** Vulnerability Impact: **Denial of Service** Risk: **Medium**

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.1
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12
http://www.kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.32.log

Other references:
http://secunia.com/advisories/15786/

Product HomePage:
http://kernel.org/

CVE Reference:
CAN-2005-1761
CAN-2005-1762
CAN-2005-1763
CAN-2005-1767
CAN-2005-1913
CAN-2005-3108
CAN-2005-3109
CVE-2005-3272

❖ 16097 Linux Kernel Insufficient address validation in "ptrace()" to crash the kernel 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.

Insufficient address validation in "ptrace()" on the AMD64 platform can be exploited to crash the kernel by setting an invalid segment base.

The vulnerability has been fixed in version 2.6.11.11.

Test Case Impact: **Gather Info** Vulnerability Impact: **Denial of Service** Risk: **Medium**

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.11
http://www.ubuntulinux.org/support/documentation/usn/usn-137-1

Other references:
http://secunia.com/advisories/15630/

Product HomePage:
http://kernel.org/

CVE Reference:
CAN-2005-0756
CAN-2005-1265
CVE Compatible

New Vulnerabilities found this Week

F-Secure Anti-Virus Archive Handling Vulnerabilities
"System access, Security Bypass"

Some vulnerabilities have been reported in various F-Secure products, which can be exploited by malware to bypass detection or malicious people to compromise a vulnerable system.

1) A boundary error in the handling of ZIP archives can be exploited via a specially crafted ZIP archive to cause a buffer overflow and execute arbitrary code.

2) An error in the scanning functionality when processing RAR and ZIP archives can be exploited to prevent malware from being detected.

The vulnerabilities affect the following products:
* F-Secure Anti-Virus for Workstation version 5.44 and earlier

* F-Secure Anti-Virus for Windows Servers version 5.52 and earlier
* F-Secure Anti-Virus for Citrix Servers version 5.52
* F-Secure Anti-Virus for MIMEsweeper version 5.61 and earlier
* F-Secure Anti-Virus Client Security version 6.01 and earlier
* F-Secure Anti-Virus for MS Exchange version 6.40 and earlier
* F-Secure Internet Gatekeeper version 6.42 and earlier
* F-Secure Anti-Virus for Firewalls version 6.20 and earlier
* F-Secure Internet Security 2004, 2005 and 2006
* F-Secure Anti-Virus 2004, 2005 and 2006
* Solutions based on F-Secure Personal Express version 6.20 and earlier
* F-Secure Anti-Virus for Linux Workstations version 4.52 and earlier
* F-Secure Anti-Virus for Linux Servers version 4.64 and earlier
* F-Secure Anti-Virus for Linux Gateways version 4.64 and earlier
* F-Secure Anti-Virus for Samba Servers version 4.62
* F-Secure Anti-Virus Linux Client Security 5.11 and earlier
* F-Secure Anti-Virus Linux Server Security 5.11 and earlier
* F-Secure Internet Gatekeeper for Linux 2.14 and earlier

Solution:
Apply patches (see patch matrix in vendor advisory).

Provided and/or discovered by:
The vendor credits Thierry Zoller.

Original Advisory:
http://www.f-secure.com/security/fsc-2006-1.shtml

Nortel Products Microsoft Windows WMF "SETABORTPROC" Code Execution
“System access”

Nortel Networks has acknowledged a potential vulnerability in various products, which can be exploited by malicious people to compromise a vulnerable system.

For more information:
SA18255

The following products are potentially affected:
* Nortel CallPilot (versions 1.07, 2.x, 3.0, and 4.0)
* Nortel Multimedia Communication Server 5100
* Nortel Multimedia Communication Server 5200

Solution:
Do not browse untrusted web sites and do not open images from untrusted sources.

Original Advisory:
http://www130.nortelnetworks.com...umentOID=375341&RenditionID=

AOL You've Got Pictures ActiveX Control Buffer Overflow
“DoS, system access”

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

The vulnerability is caused due to a boundary error in the YPG Picture Finder Tool ActiveX Control (YGPPicFinder.DLL). This can be exploited to cause a buffer overflow and may allow arbitrary code execution.

The vulnerability has been reported in AOL 8.0, 8.0 Plus, and 9.0 Classic. The vulnerable control was also distributed via the You've Got Pictures website prior to 2004.

Solution:
Update to AOL 9.0 Optimized and AOL 9.0 Security Edition or apply hotfix.
http://download.newaol.com/security/YGPClean.exe

Provided and/or discovered by:
The vendor credits Richard M. Smith.

Original Advisory:
US-CERT VU#715730:
http://www.kb.cert.org/vuls/id/715730

Novell Open Enterprise Server Remote Manager Buffer Overflow
“System access”

A vulnerability has been reported in Novell Open Enterprise Server Remote Manager, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an error in the handling of a HTTP POST request with a negative "Content-Length" header. This can be exploited to cause a heap-based buffer overflow.

Successful exploitation allows arbitrary code execution.

Solution:
Apply updates.

Updates are available via Red Carpet / ZLM or from the maintenance web:

http://support.novell.com/cgi-bi...0a99a736eb966cc0e52fb71ee98.html
http://portal.suse.com/psdb/1af470a99a736eb966cc0e52fb71ee98.html

Provided and/or discovered by:
Discovered by anonymous person and reported via iDEFENSE.

Changelog:
2006-01-19: Updated link to vendor advisory.

Original Advisory:
Novell:
http://www.novell.com/linux/security/advisories/2006_02_novellnrm.html

iDEFENSE:
http://www.idefense.com/intellig...lnerabilities/display.php?id=371

Oracle Products Multiple Vulnerabilities and Security Issues
“Manipulation of data, Exposure of system information, Exposure of sensitive information”

82 vulnerabilities and security issues have been reported in various Oracle products. Some have

an unknown impact, and others can be exploited to gain knowledge of certain information, overwrite arbitrary files, and to conduct SQL injection attacks.

Details have been disclosed for the following vulnerabilities:

1) Input passed to various parameters in the procedures within the DBMS_DATAPUMP, DBMS_REGISTRY, DBMS_CDC_UTILITY, DBMS_CDC_PUBLISH, DBMS_METADATA_UTIL, DBMS_METADATA_INT, DBMS_METADATA, CTXSYS.DRILOAD, CTXSYS.DRIDML, CTXSYS.CTX_DOC, CTXSYS.CTX_QUERY, and CATINDEXMETHODS Oracle PL/SQL packages is not properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

2) Input passed to various parameters in the ATTACH_JOB, HAS_PRIVS, and OPEN_JOB procedures within the SYS.KUPV$FT package is not properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

The vulnerabilities have been reported in Oracle 10g Release 1.

3) Input passed to various parameters in several procedures within the SYS.KUPV$FT_INT package is not properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

The vulnerabilities have been reported in Oracle 10g Release 1.

4) Design errors in the Oracle Database causes the Oracle TDE (Transparent Data Encryption) wallet password to be logged in cleartext, and the masterkey for the TDE wallet to be stored unencrypted.

The security issues have been reported in Oracle Database 10g Release 2 version 10.2.0.1.

5) Some errors in the Reports component of the Oracle Application Server can be exploited to read parts of any files or overwrite any files via Oracle Reports.

For more information, see #2, #3, and #4 in:
SA16092

The vulnerability has been reported in versions 1.0.2.0 through 10.1.0.2.

6) Input passed to the AUTH_ALTER_SESSION attribute in a TNS authentication message is not properly sanitised before being used in an SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

Successful exploitation allows execution of arbitrary SQL queries with SYS user privileges.

The vulnerability has been reported in Oracle 8i (8.1.7.x.x), Oracle 9i (9.2.0.7), Oracle 10g Release 1 (10.1.0.4.2), and Oracle 10g Release 2 (10.2.0.1.0).

The following supported products are affected by one or more of the 82 vulnerabilities:
* Oracle Database 10g Release 2, version 10.2.0.1
* Oracle Database 10g Release 1, versions 10.1.0.3, 10.1.0.4, 10.1.0.5
* Oracle9i Database Release 2, versions 9.2.0.6, 9.2.0.7
* Oracle8i Database Release 3, version 8.1.7.4
* Oracle Enterprise Manager 10g Grid Control, versions 10.1.0.3, 10.1.0.4
* Oracle Application Server 10g Release 2, versions 10.1.2.0.0, 10.1.2.0.1, 10.1.2.0.2, 10.1.2.1.0
* Oracle Application Server 10g Release 1 (9.0.4), versions 9.0.4.1, 9.0.4.2
* Oracle Collaboration Suite 10g Release 1, versions 10.1.1, 10.1.2
* Oracle9i Collaboration Suite Release 2, version 9.0.4.2
* Oracle E-Business Suite Release 11i, versions 11.5.1 through 11.5.10 CU2
* Oracle E-Business Suite Release 11.0
* PeopleSoft Enterprise Portal, versions 8.4, 8.8, 8.9
* JD Edwards EnterpriseOne Tools, OneWorld Tools, versions 8.95.F1, SP23_L1

Solution:
Apply patches (see vendor advisory).

Provided and/or discovered by:
1-5) Alexander Kornbrust, Red Database Security.
6) Amichai Shulman

Changelog:
2006-01-19: Updated link in "Original Advisory". Added link to US-CERT vulnerability note.
2006-01-20: Added CVE references. Updated "Description" section.

Original Advisory:

Oracle:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html

Red Database Security:
http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html
http://www.red-database-security.../oracle_tde_wallet_password.html
http://www.red-database-security.../oracle_tde_unencrypted_sga.html
http://www.red-database-security...racle_sql_injection_kupv$ft.html
http://www.red-database-security...e_sql_injection_kupv$ft_int.html
http://www.red-database-security..._reports_overwrite_any_file.html
http://www.red-database-security...e_reports_read_any_xml_file.html

Imperva:
http://www.imperva.com/applicati...papers/oracle-dbms-01172006.html

Other References:
SA16092:
http://secunia.com/advisories/16092/

US-CERT VU#545804:
http://www.kb.cert.org/vuls/id/545804

KDE kjs UTF-8 Encoded URI Buffer Overflow Vulnerability

“System access, DoS”

Maksim Orlovich has reported a vulnerability in KDE kjs, which can be exploited by malicious people to cause a DoS (Denial of Service) or to compromise a user's system.

The vulnerability is caused due to a boundary error in kjs in the decoding of UTF-8 encoded URI sequences. This can be exploited to cause a heap-based buffer overflow by supplying specially crafted JavaScript code via an application using the affected JavaScript interpreter engine (e.g. Konqueror).

Successful exploitation allows execution of arbitrary code.

The vulnerability has been reported in versions 3.2.0 through 3.5.0.

Solution:

Apply patches.

KDE 3.4.0 - 3.5.0:

ftp://ftp.kde.org/pub/kde/security_patches/post-3.4.3-kdelibs-kjs.diff

ecc0ec13ce3b06e94e35aa8e937e02bf

KDE 3.2.0 - 3.3.2:

ftp://ftp.kde.org/pub/kde/security_patches/post-3.2.3-kdelibs-kjs.diff

9bca9b44ca2d84e3b2f85ffb5d30e047

Provided and/or discovered by:

Maksim Orlovich

Original Advisory:

http://www.kde.org/info/security/advisory-20060119-1.txt

ELOG Format String and Directory Traversal Vulnerabilities

“Security Bypass, DoS, System access”

Some vulnerabilities have been reported in ELOG, which can be exploited by malicious people to cause a DoS (Denial of Service), bypass certain security restrictions, and potentially compromise a vulnerable system.

1) A format string error exists in the "write_logfile()" function in elogd.c when logging events to the log file. This can be exploited to crash the server and may allow arbitrary code execution via a specially-crafted username submitted from the login page.

Successful exploitation requires that logging is enabled.

2) An error in the validation of certain URLs may be exploited to access files from outside of the elog directory via requests containing the "../.." sequence in a directory traversal attack.

The vulnerabilities have been reported in versions prior to 2.6.1.

NOTE: Several other unspecified issues, which may be security related, have also been fixed.

Solution:
Update to version 2.6.1.
http://midas.psi.ch/elog/download.html

Provided and/or discovered by:
Reported by vendor.

Original Advisory:
http://midas.psi.ch/elog/download/ChangeLog

Light Weight Calendar "date" PHP Code Execution Vulnerability

“System access”

Aliaksandr Hartsuyeu has reported a vulnerability in Light Weight Calendar, which can be exploited by malicious people to compromise a vulnerable system.

Input passed to the "date" parameter in "index.php" isn't properly sanitised before being used in an "eval()" call. This can be exploited to execute arbitrary PHP code.

Example:
http://[victim]/index.php?stam=1928504&date=20050901);[code]&View=month

The vulnerability has been reported in version 1.0. Other versions may also be affected.

Solution:
Edit the source code to ensure that input is properly sanitised.

Provided and/or discovered by:
Aliaksandr Hartsuyeu

Original Advisory:
http://evuln.com/vulns/29/summary.html

WebspotBlogging "username" SQL Injection Vulnerability

“System access, Manipulation of data, Security Bypass”

Aliaksandr Hartsuyeu has discovered a vulnerability in WebspotBlogging, which can be exploited by malicious people to conduct SQL injection attacks and potentially compromise a vulnerable system.

Input passed to the "username" parameter in "login.php" isn't properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

Successful exploitation requires that "magic_quotes_gpc" is disabled.

This can further be exploited to bypass the authentication process and access the administration section where PHP code reportedly can be injected via the "Import Themes" functionality.

The vulnerability has been confirmed in version 3.0. Other versions may also be affected.

Solution:

Edit the source code to ensure that input is properly sanitised.

Provided and/or discovered by:

Aliaksandr Hartsuyeu

Original Advisory:

http://evuln.com/vulns/41/summary.html

Vulnerability Resource

Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the ‘security portal for information system security professionals’ is well founded.

http://www.infosyssec.org/infosyssec/

Thank You

Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at ScoutNews@netVigilance.com.

About SecureScout
SecureScout is a leading vulnerability scanner and management tool developed and marketed worldwide by NexantiS Corporation.
SecureScout is a trademark of NexantiS Corporation.
netVigilance, Inc. is a partner of NexantiS and an authorized distributor of SecureScout.

For any inquiry about SecureScout by:
Customers in America and Northern Europe contact us at info@netVigilance.com
Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at info-scanner@securescout.net