netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 17 April 28, 2006

Table of Contents

Product Focus

Task Scheduler Vulnerability Scanner – Another of our Free single vulnerability scanners will check for Microsoft Task Scheduler vulnerability.

This Week in Review

A "Rocket Scientist" launches Ransomware, White Hat ends up in hot water over USC breach and password overloading causes vulnerabilities.

Enjoy reading

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

Top Security News Stories this Week

- **'Ransom' Trojan hits net**

Sophos issued a warning about a new Trojan in the wild which they are calling Troj/Ransom-A. This fairly new form of Malware infects the computer then displays a message that the Virus will start deleting files every 30 minutes until the infected user wires (get this) $10.99 via Western Union.

The Hacker also provides technical support in case the unlocking procedure doesn't work. (I wonder why hasn't this guy landed a real job? – *Ed.*)

PCWorld

Full Story :

http://news.yahoo.com/s/pcworld/20060427/tc_pcworld/125569

- **Security "Professional" may have inadvertently caused recent USC break-in.**

U.S. Attorney's Office in the Central District of California leveled a single charge of computer intrusion against San Diego-based information-technology professional Eric McCarty. While researching a vulnerability without the school's permission, he allegedly breached a university's online application system. This action may have a hacker to break-in recently and make off with SSNs and data on 275,000 students.

The indignant McCarty is now advising white hats to "keep vulnerabilities to yourself" since his run-in with the FBI. My advice would to get permission first then release flaws through proper channels – *Ed*.

Free Republic

Full Story :

http://www.freerepublic.com/focus/f-news/1622571/posts

- **Password overload causing security concerns**

PriceWaterhouse-Cooper recently found that cyber-attacks are costing corporations 50 percent more than the level calculated two years ago, one of the primary concerns is weak passwords. With users required to remember more and more passwords, they often resort to using the same one for most of their authentications. This practice make password cracking like a prarie fire once the hacker has learned on password this will most likely give them access to all of the users accounts.

Reuters

Related Links :
http://today.reuters.com/news/articlenews.aspx?type=technologyNews&storyid=2006-04-25T112102Z_01_L24471820_RTRUKOC_0_US-CRIME-BRITAIN-TECHNOLOGY.xml

New Vulnerabilities Tested in SecureScout

- **13364 Oracle Database Server - Oracle Spatial component SQL Injection vulnerability (apr-2006/DB11)**

An SQL injection vulnerability in the Oracle Spatial component may allow a remote attacker to execute arbitrary SQL commands on a vulnerable Oracle installation.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2006.html
http://www.us-cert.gov/cas/techalerts/TA06-109A.html
http://secunia.com/advisories/19712/

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

CVE Reference: CVE-2006-1875

- **13365 Oracle Database Server - Oracle Spatial component SQL Injection vulnerability (apr-2006/DB12)**

An SQL injection vulnerability in the Oracle Spatial component may allow a remote attacker to execute arbitrary SQL commands on a vulnerable Oracle installation.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2006.html
http://www.us-cert.gov/cas/techalerts/TA06-109A.html
http://www.kb.cert.org/vuls/id/240249
http://secunia.com/advisories/19712/

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

CVE Reference: CVE-2006-1876

- **13366 Oracle Database Server - Oracle Spatial component unspecified vulnerability (apr-2006/DB13)**

An unspecified vulnerability in the Oracle Spatial component may allow a remote attacker to compromise system integrity and availability.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html

Other references:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2006.html
http://www.us-cert.gov/cas/techalerts/TA06-109A.html
http://www.kb.cert.org/vuls/id/240249
http://secunia.com/advisories/19712/

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

CVE Reference: CVE-2006-1877

❖ 16210 Linux Kernel Program Control Return Denial of Service

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

The vulnerability is caused due to an error when the kernel returns program control using SYSRET on Intel EM64T CPUs. The may cause a DoS due to the way Intel EM64T CPUs handle uncanonical return addresses when a user has been able to change the frames.

The vulnerability has been reported in versions 2.6 through 2.6.16.5 not included.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.5

Other references:
* SECUNIA:19639
* URL:http://secunia.com/advisories/19639

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-0744

❖ 16211 Linux Kernel x87 Register Information Leak

A security issue has been reported in Linux Kernel, which can be exploited by malicious, local users to gain knowledge of potentially sensitive information.

The problem is caused due to AMD K7/K8 CPUs only saving/restoring certain x87 registers in FXSAVE instructions when an exception is pending. This may leak x87 register information between processes.

The vulnerability has been reported in versions 2.6 through 2.6.16.9 not included

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.9

Other references:
* FREEBSD:FreeBSD-SA-06:14
* URL:ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:14.fpu.asc
* MISC:http://security.freebsd.org/advisories/FreeBSD-SA-06:14-amd.txt
* CONFIRM:https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=187910
* CONFIRM:https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=187911
* MLIST:[linux-kernel] 20060419 RE: Linux 2.6.16.9
* URL:http://marc.theaimsgroup.com/?l=linux-kernel&m=114548768214478&w=2
* BID:17600
* URL:http://www.securityfocus.com/bid/17600
* FRSIRT:ADV-2006-1426
* URL:http://www.frsirt.com/english/advisories/2006/1426
* SECUNIA:19724
* URL:http://secunia.com/advisories/19724
* SECUNIA:19715
* URL:http://secunia.com/advisories/19715

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-1056

❖ 16212 Linux Kernel Shared Memory Restrictions Bypass

A vulnerability has been reported in Linux Kernel, which can be exploited by malicious, local users to bypass certain security restrictions.

The vulnerability is caused due to the "mprotect()" function giving write permissions to read-only attachments of shared memory regardless of the permissions given by IPC.

The vulnerability has been reported in versions 2.6 through 2.6.16.7 not included.

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

References:

Original advisory:

http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.6

Other references:
* BID:17587
* URL:http://www.securityfocus.com/bid/17587
* SECUNIA:19664
* URL:http://secunia.com/advisories/19664
* SECUNIA:19657
* URL:http://secunia.com/advisories/19657

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-1524

❖ 16213 Linux Kernel "ip_route_input()" Denial of Service Vulnerability

A vulnerability has been reported in 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 error in the "ip_route_input()" function when the route is requested for a multi-cast IP address.

The vulnerability has been reported in versions 2.6 through 2.6.16.8 not included.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.8

Other references:
* CONFIRM:https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=189346
* BID:17593
* URL:http://www.securityfocus.com/bid/17593
* FRSIRT:ADV-2006-1399
* URL:http://www.frsirt.com/english/advisories/2006/1399
* SECUNIA:19709
* URL:http://secunia.com/advisories/19709

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-1525

❖ 16214 Linux Kernel perfmon Local Denial of Service Vulnerability

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

The vulnerability is caused due to an error in perfmon (perfmon.c) during exit

processing and may cause a crash when a task is interrupted while another process is accessing the "mm_struct" structure.

The vulnerability has been reported in versions 2.6 through 2.6.16.12 not included.

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

References:

Original advisory:
* MLIST:[linux-ia64] [PATCH 1/1] ia64: perfmon.c trips BUG_ON in put_page_testzero
* URL:http://marc.theaimsgroup.com/?l=linux-ia64&m=113882384921688

Other references:
* CONFIRM:https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=185082
* BID:17482
* URL:http://www.securityfocus.com/bid/17482

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-0558

❖ 16215 Internet Explorer "mhtml:" Redirection Disclosure of Sensitive Information (Remote File Checking)

codedreamer has discovered a vulnerability in Internet Explorer, which can be exploited by malicious people to disclose potentially sensitive information.

The vulnerability is caused due to an error in the handling of redirections for URLs with the "mhtml:" URI handler. This can be exploited to access documents served from another web site.

The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2. Other versions may also be affected.

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

References:

Original advisory:
http://secunia.com/advisories/19738/

Product Homepage:
http://www.microsoft.com/windows/ie/default.mspx

CVE Reference: None

❖ 16216 Internet Explorer "object" Tag Memory Corruption Code Execution (Remote File Checking)

Michal Zalewski has discovered a vulnerability in Internet Explorer, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error in the processing of certain sequences of nested "object" HTML tags. This can be exploited to corrupt memory by tricking a user into visiting a malicious web site.

Successful exploitation allows execution of arbitrary code.

The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2. Other versions may also be affected.

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/archive/1/431796/100/0/threaded

Other references:
* BUGTRAQ:20060422 MSIE (mshtml.dll) OBJECT tag vulnerability
* URL:http://www.securityfocus.com/archive/1/archive/1/431796/100/0/threaded
* FULLDISC:20060422 Re: MSIE (mshtml.dll) OBJECT tag vulnerability
* URL:http://archives.neohapsis.com/archives/fulldisclosure/2006-04/0616.html
* FRSIRT:ADV-2006-1507
* URL:http://www.frsirt.com/english/advisories/2006/1507
* SECUNIA:19762
* URL:http://secunia.com/advisories/19762

Product Homepage:
http://www.microsoft.com/windows/ie/default.mspx

CVE Reference: CVE-2006-1992

New Vulnerabilities found this Week

Internet Explorer "object" Tag Memory Corruption Code Execution
"Corrupt memory; execution of arbitrary code"

Michal Zalewski has discovered a vulnerability in Internet Explorer, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error in the processing of certain sequences of nested "object" HTML tags. This can be exploited to corrupt memory by tricking a user into visiting a malicious web site.

Successful exploitation allows execution of arbitrary code.

The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2. Other versions may also be affected.

References:

http://lists.grok.org.uk/pipermail/full-disclosure/2006-April/045422.html
http://descriptions.securescout.com/tc/16216

Oracle Database "DBMS_EXPORT_EXTENSION" Package SQL Injection
"SQL injection attacks"

David Litchfield has reported a vulnerability in Oracle Database, which can be exploited by malicious users to conduct SQL injection attacks.

The vulnerability is caused due to an unspecified input validation error in the "DBMS_EXPORT_EXTENSION" package. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

The vulnerability has been reported in Oracle Database 10g Release 2 with the April 2006 Critical Patch Update. Other versions may also be affected.

References:
http://lists.grok.org.uk/pipermail/full-disclosure/2006-April/045540.html

xine-lib MPEG Stream Handling Buffer Overflow Vulnerability
"Arbitrary code execution"

Federico L. Bossi Bonin has reported a vulnerability in xine-lib, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is cause due to a boundary error within the handling of MPEG streams. This can be exploited to cause a buffer overflow and may allow arbitrary code execution via a specially-crafted MPEG file.

The vulnerability has been reported in libxine 1.14 that is distributed in xine-lib 1.1.1. Other versions may also be affected.

References:
http://milw0rm.com/exploits/1641

Internet Explorer "mhtml:" Redirection Disclosure of Sensitive Information
"Disclose potentially sensitive information"

codedreamer has discovered a vulnerability in Internet Explorer, which can be exploited by malicious people to disclose potentially sensitive information.

The vulnerability is caused due to an error in the handling of redirections for URLs with the "mhtml:" URI handler. This can be exploited to access documents served from another web site.

The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2. Other versions may also be affected.

References:
http://secunia.com/advisories/19738/
http://descriptions.securescout.com/tc/16215

PowerDNS Recursor Denial of Service Vulnerability
"Denial of Service"

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

The vulnerability is caused due to an error in the recursor when parsing certain DNS packets. This can be exploited to crash the recursor via a malformed EDNS0 packet.

The vulnerability has been reported in versions prior to 3.0.1.

References:
http://doc.powerdns.com/changelog.html#CHANGELOG-RECURSOR-3-0-1

pdnsd DNS Query Handling Memory Leak Vulnerability
"Denial of Service"

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

The vulnerability is caused due to a memory leak error within the handling of the QTYPE and QCLASS DNS queries. This can be exploited to cause pdnsd to consume large amount of memory, thus causing it to crash or cause the system to become unstable.

The vulnerability has been reported in versions prior to 1.2.4.

References:
http://www.niscc.gov.uk/niscc/docs/re-20060425-00312.pdf?lang=en

BIND Zone Transfer TSIG Handling Denial of Service
"Denial of Service**"**

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

The vulnerability is caused due to an error within the handling of the TSIG in the second or subsequent messages in a zone transfer. This can be exploited to crash "named" via a malformed TSIG in the messages.

Successful exploitation requires that the first zone transfer message have a valid TSIG.

References:
http://www.niscc.gov.uk/niscc/docs/re-20060425-00312.pdf?lang=en

Ethereal Multiple Protocol Dissector Vulnerabilities
"Denial of Service"

Multiple vulnerabilities have been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

The vulnerabilities are caused due to various types of errors including boundary errors, an off-by-one error, an infinite loop error, and several unspecified errors in a multitude of protocol dissectors.

Successful exploitation causes Ethereal to stop responding, consume a large amount of system resources, crash, or execute arbitrary code.

The vulnerabilities affect versions 0.8.5 through 0.10.14.

References:
http://www.ethereal.com/docs/release-notes/ethereal-0.99.0.html
http://www.ethereal.com/appnotes/enpa-sa-00023.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.