netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 13

March 28, 2008

Table of Contents

Product Focus

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

Jesper Jurcenoks of netVigilance is keynote speaker at ITEC's "Master Mind Panel and Lunch: Security for Second Circle Technologies", the first in Houston May 7-8, see **http://www.netvigilance.com/events**

This Week in Review

These are the worries of Microsoft's chief security advisor. Some advice on how-to encrypt your data. Security needs in the virtual environment. New rootkit variant discovered.

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

- ### What spooks Microsoft's chief security advisor

Application exploits, virtualization security are big concerns
Microsoft's U.S. general manager/chief security advisor for its National Security Team

thinks like a true security professional: In every bit of good news, Bret Arsenault wonders what bad news could be lurking behind it.

Speaking at the Boston SecureWorld conference Wednesday, the 19-year Microsoft veteran whose job includes protecting enterprises, developers and Microsoft itself said there actually is plenty of good news on the security front. For example, his outfit scans a half million devices (with customer permission) per month and in the first half of last year saw the first period-over-period decline in new vulnerabilities disclosed across Microsoft and non-Microsoft software since 2003.

networkworld

Full Story :
http://www.networkworld.com/news/2008/032608-microsoft-security-concerns.html?fsrc=netflash-rss

❖ A guide to practical encryption across the business

There is only one thing worse than realising that you have left your laptop in the back of a taxi. That is the recollection that you have not encrypted any of the data on it - including all of your contact information, your sensitive e-mails, all of your online passwords, and that spreadsheet full of customer names and addresses. That sort of situation spells trouble for your customers, your company and, ultimately, for you. Unfortunately, this kind of thing happens more often than you would think, in both the public and private sectors. In January, the government faced a storm of criticism after a navy officer's laptop containing the details of 600,000 people was stolen. The data, including passport numbers, bank details and national insurance numbers, was unencrypted. In December, the DVLA lost discs en route to its headquarters in Swansea that contained unencrypted information on 6,000 drivers.

computerweekly

Full Story :
http://www.computerweekly.com/Articles/2008/03/25/229965/a-guide-to-practical-encryption-across-the-business.htm

❖ Virtual Appliances: A Safety Zone in the Virtual Environment

Virtualized applications are easy to install and upload. "I did a demo for a large bank in the U.S. and the guy asked me how are we deploying it so I went through the deployment process, deployed our product on a host with 15 servers and got it up and running with full protection in five minutes," said Hezi Moore, founder of Reflex Systems. As corporations increasingly virtualize their environments, they are finding that traditional physical security Free Trial. Security Software As A Service From Webroot. and network applications are not adequate for their needs.

"Most network security solutions are based on custom-made ASICs (application-specific integrated circuits) running customized software, and don't provide adequate security in a virtual environment," Mark Boltz, senior solutions architect at Stonesoft, told TechNewsWorld.

technewsworld

Full Story :
http://www.technewsworld.com/story/software/62273.html

❖ Researchers Discover Rootkit Variation

While there might not be new malicious threats under the sun, there are plenty of new ways to spin old virus attacks. Trend Micro researchers discovered last weekend a new variation of a MBR rootkit released in the wild, which contains new technology to prevent detection.

When combined with Web threats, the new rootkit is proving to be both a destructive and prolific combination, security experts say.

The rootkit models a similar virus from several years ago but with one added twist -- the ability to circumvent a lot of anti-rootkit software and remain undetected.

"It's a spin on an old attack," said Jamz Yaneza, research project manager for Trend Micro. "This is typical of virus writers and mothership authors trying to find ways and means to make it more difficult."

crn

Full Story :
http://www.crn.com/security/206905724;jsessionid=UW05QDFZCIFJCQSNDLRSKHSCJUNN2JVN

New Vulnerabilities Tested in SecureScout

❖ 16730 Oracle Application Server - OC4J component unspecified Vulnerability (jul-2006/AS09)

An unspecified vulnerability with unknown impact exists in Oracle Application Server OC4J component.

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

Some References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/440758/100/100/threaded
* CERT: TA06-200A
http://www.us-cert.gov/cas/techalerts/TA06-200A.html
* BID: 19054
http://www.securityfocus.com/bid/19054

* FRSIRT: ADV-2006-2863
http://www.frsirt.com/english/advisories/2006/2863
* FRSIRT: ADV-2006-2947
http://www.frsirt.com/english/advisories/2006/2947
* SECTRACK: 1016529
http://securitytracker.com/id?1016529
* SECUNIA: 21111
http://secunia.com/advisories/21111
* SECUNIA: 21165
http://secunia.com/advisories/21165
* XF: oracle-cpu-july-2006(27897)
http://xforce.iss.net/xforce/xfdb/27897

CVE Reference: CVE-2006-3713

❖ 16731 Oracle Application Server - OC4J component unspecified Vulnerability (jul-2006/AS10)

An unspecified vulnerability with unknown impact exists in Oracle Application Server OC4J component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/440758/100/100/threaded
* CERT: TA06-200A
http://www.us-cert.gov/cas/techalerts/TA06-200A.html
* BID: 19054
http://www.securityfocus.com/bid/19054
* FRSIRT: ADV-2006-2863
http://www.frsirt.com/english/advisories/2006/2863
* FRSIRT: ADV-2006-2947
http://www.frsirt.com/english/advisories/2006/2947
* SECTRACK: 1016529
http://securitytracker.com/id?1016529
* SECUNIA: 21111
http://secunia.com/advisories/21111
* SECUNIA: 21165
http://secunia.com/advisories/21165
* XF: oracle-cpu-july-2006(27897)
http://xforce.iss.net/xforce/xfdb/27897

CVE Reference: CVE-2006-3714

❖ 16736 Oracle Application Server - ModPL/SQL for Apache component unspecified Vulnerability (apr-2006/PLSQL01)

An unspecified vulnerability with unknown impact exists in Oracle Application Server ModPL/SQL for Apache component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html

CVE Reference:

❖ 16739 Oracle Application Server - Portal component unspecified Vulnerability (jan-2006/AS01)

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
* CERT-VN: VU#545804
http://www.kb.cert.org/vuls/id/545804
* BID: 16287
http://www.securityfocus.com/bid/16287
* FRSIRT: ADV-2006-0243
http://www.frsirt.com/english/advisories/2006/0243
* FRSIRT: ADV-2006-0323
http://www.frsirt.com/english/advisories/2006/0323
* SECTRACK: 1015499
http://securitytracker.com/id?1015499
* SECUNIA: 18493
http://secunia.com/advisories/18493
* SECUNIA: 18608
http://secunia.com/advisories/18608
* XF: oracle-january2006-update(24321)
http://xforce.iss.net/xforce/xfdb/24321

CVE Reference: CVE-2006-0273

❖ 16740 Oracle Application Server - Java Net component unspecified Vulnerability (jan-2006/JN01)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Java Net component.

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

References:

* BUGTRAQ: 20080103 rPSA-2008-0004-1 tshark wireshark
http://www.securityfocus.com/archive/1/archive/1/485792/100/0/threaded
* MISC:
http://bugs.gentoo.org/show_bug.cgi?id=199958
* CONFIRM:
http://www.wireshark.org/security/wnpa-sec-2007-03.html
* CONFIRM:
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0004
* CONFIRM:
https://issues.rpath.com/browse/RPL-1975
* GENTOO: GLSA-200712-23
http://security.gentoo.org/glsa/glsa-200712-23.xml
* MANDRIVA: MDVSA-2008:001
http://www.mandriva.com/security/advisories?name=MDVSA-2008:001
* MANDRIVA: MDVSA-2008:1
http://www.mandriva.com/security/advisories?name=MDVSA-2008:1
* REDHAT: RHSA-2008:0058
http://www.redhat.com/support/errata/RHSA-2008-0058.html
* SUSE: SUSE-SR:2008:004
http://lists.opensuse.org/opensuse-security-announce/2008-02/msg00008.html
* BID: 27071
http://www.securityfocus.com/bid/27071
* SECUNIA: 28288
http://secunia.com/advisories/28288
* SECUNIA: 27777
http://secunia.com/advisories/27777
* SECUNIA: 28304
http://secunia.com/advisories/28304
* SECUNIA: 28325
http://secunia.com/advisories/28325
* SECUNIA: 28564
http://secunia.com/advisories/28564
* SECUNIA: 29048
http://secunia.com/advisories/29048
* XF: wireshark-wimax-dissector-dos(39183)
http://xforce.iss.net/xforce/xfdb/39183

CVE Reference: CVE-2007-6441

❖ 16741 Oracle Application Server - Oracle HTTP Server component unspecified Vulnerability (jan-2006/OHS01)

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
* CERT-VN: VU#545804
http://www.kb.cert.org/vuls/id/545804
* BID: 16287
http://www.securityfocus.com/bid/16287
* FRSIRT: ADV-2006-0243
http://www.frsirt.com/english/advisories/2006/0243
* FRSIRT: ADV-2006-0323
http://www.frsirt.com/english/advisories/2006/0323
* SECTRACK: 1015499
http://securitytracker.com/id?1015499
* SECUNIA: 18493
http://secunia.com/advisories/18493
* SECUNIA: 18608
http://secunia.com/advisories/18608
* XF: oracle-january2006-update(24321)
http://xforce.iss.net/xforce/xfdb/24321

CVE Reference: CVE-2006-0286

❖ 16742 Oracle Application Server - Oracle HTTP Server component unspecified Vulnerability (jan-2006/OHS02)

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
* CERT-VN: VU#545804
http://www.kb.cert.org/vuls/id/545804
* BID: 16287
http://www.securityfocus.com/bid/16287
* FRSIRT: ADV-2006-0243
http://www.frsirt.com/english/advisories/2006/0243
* FRSIRT: ADV-2006-0323
http://www.frsirt.com/english/advisories/2006/0323
* SECTRACK: 1015499
http://securitytracker.com/id?1015499
* SECUNIA: 18493
http://secunia.com/advisories/18493
* SECUNIA: 18608

http://secunia.com/advisories/18608
* XF: oracle-january2006-update(24321)
http://xforce.iss.net/xforce/xfdb/24321

CVE Reference: CVE-2006-0287

❖ 16743 Oracle Application Server - Oracle Forms component unspecified Vulnerability (jan-2006/FORM01)

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
* CERT-VN: VU#545804
http://www.kb.cert.org/vuls/id/545804
* BID: 16287
http://www.securityfocus.com/bid/16287
* FRSIRT: ADV-2006-0243
http://www.frsirt.com/english/advisories/2006/0243
* FRSIRT: ADV-2006-0323
http://www.frsirt.com/english/advisories/2006/0323
* SECTRACK: 1015499
http://securitytracker.com/id?1015499
* SECUNIA: 18493
http://secunia.com/advisories/18493
* SECUNIA: 18608
http://secunia.com/advisories/18608
* XF: oracle-january2006-update(24321)
http://xforce.iss.net/xforce/xfdb/24321

CVE Reference: CVE-2006-0284

❖ 16744 Oracle Application Server - Oracle Forms component unspecified Vulnerability (jan-2006/FORM02)

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
* CERT-VN: VU#545804
http://www.kb.cert.org/vuls/id/545804
* BID: 16287

http://www.securityfocus.com/bid/16287
* FRSIRT: ADV-2006-0243
http://www.frsirt.com/english/advisories/2006/0243
* FRSIRT: ADV-2006-0323
http://www.frsirt.com/english/advisories/2006/0323
* SECTRACK: 1015499
http://securitytracker.com/id?1015499
* SECUNIA: 18493
http://secunia.com/advisories/18493
* SECUNIA: 18608
http://secunia.com/advisories/18608
* XF: oracle-january2006-update(24321)
http://xforce.iss.net/xforce/xfdb/24321

CVE Reference: CVE-2006-0284

❖ 16745 Oracle Application Server - Oracle Reports Developer component unspecified Vulnerability (jan-2006/REP01)

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
* CERT-VN: VU#545804
http://www.kb.cert.org/vuls/id/545804
* BID: 16287
http://www.securityfocus.com/bid/16287
* FRSIRT: ADV-2006-0243
http://www.frsirt.com/english/advisories/2006/0243
* FRSIRT: ADV-2006-0323
http://www.frsirt.com/english/advisories/2006/0323
* SECTRACK: 1015499
http://securitytracker.com/id?1015499
* SECUNIA: 18493
http://secunia.com/advisories/18493
* SECUNIA: 18608
http://secunia.com/advisories/18608
* XF: oracle-january2006-update(24321)
http://xforce.iss.net/xforce/xfdb/24321

CVE Reference: CVE-2006-0288

New Vulnerabilities found this Week

Mozilla Firefox Multiple Vulnerabilities

“Bypass certain security restrictions; Disclose sensitive information; Cross-site scripting”

Some vulnerabilities and weaknesses have been reported in Mozilla Firefox, which can be exploited by malicious people to bypass certain security restrictions, disclose potentially sensitive information, conduct cross-site scripting and phishing attacks, and potentially compromise a user's system.

1) An unspecified error in the handling of "XPCNativeWrappers" can lead to the execution of arbitrary Javascript code with the user's privileges via "setTimeout()" calls.

2) Various errors in the handling of Javascript code can be exploited to conduct cross-site scripting attacks or execute arbitrary code.

3) Various errors in the layout engine can be exploited to cause a memory corruption.

4) Various errors in the Javascript engine can be exploited to cause a memory corruption.

Successful exploitation of these vulnerabilities may allow execution of arbitrary code.

5) An error within the handling of HTTP "Referer:" headers sent with requests to URLs containing "Basic Authentication" credentials having an empty username can be exploited to bypass cross-site request forgery protections.

6) The problem is that Firefox offers a previously configured private SSL certificate when establishing connections to webservers requesting SSL Client Authentication. This can potentially be exploited to disclose sensitive information via a malicious webserver.

7) An error in the handling of the "jar:" protocol can be exploited to establish connections to arbitrary ports on the local machine.

8) An error when displaying XUL pop-up windows can be exploited to hide the window's borders and facilitate phishing attacks.

The vulnerabilities are reported in versions prior to 2.0.0.13.

References:
http://www.mozilla.org/security/announce/2008/mfsa2008-14.html
http://www.mozilla.org/security/announce/2008/mfsa2008-15.html
http://www.mozilla.org/security/announce/2008/mfsa2008-16.html
http://www.mozilla.org/security/announce/2008/mfsa2008-17.html
http://www.mozilla.org/security/announce/2008/mfsa2008-18.html
http://www.mozilla.org/security/announce/2008/mfsa2008-19.html

OpenSSH X11 Forwarding Information Disclosure Vulnerability

“Disclose sensitive information”

A vulnerability has been discovered in OpenSSH, which can be exploited by malicious, local users to disclose sensitive information.

The vulnerability is caused due to sshd improperly binding TCP ports on the local IPV6 interface if required ports on the IPV4 interface are in use. This can be exploited by a malicious, local user to intercept an X11 forwarding session by listening to a port used by sshd to forward the local X11 display (e.g. port 6010/TCP).

The vulnerability is reported in versions 4.3p2 and confirmed in 4.7p1. Other versions may also be affected.

References:
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011

Sun SPARC Enterprise T5120 and T5220 Servers Insecure Configuration

"Insecure Configuration"

A security issue has been reported in some Sun SPARC Enterprise T5120 and T5220 Servers, which can be exploited by malicious users to bypass certain security restrictions

The problem is that servers with datecode prior to BEL07480000 were shipped with an insecure Solaris 10 configuration.

The security issue only affects Sun SPARC Enterprise T5120 and T5220 Servers with datecode prior to BEL07480000.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-66-231244-1

VLC Media Player "MP4_ReadBox_rdrf()" Buffer Overflow Vulnerability

"Execution of arbitrary code"

A vulnerability has been reported in VLC Media Player, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an integer overflow error within "MP4_ReadBox_rdrf()" in modules/demux/mp4/libmp4.c and can be exploited to cause a heap-based buffer overflow via e.g. a MP4 file with a specially crafted RDRF atom.

Successful exploitation may allow execution of arbitrary code.

The vulnerability is reported in version 0.8.6e. Other versions may also be affected.

References:
http://trac.videolan.org/vlc/changeset/09572892df7e72c0d4e598c0b5e076cf330d8b0a

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