netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 4

January 25, 2008

Table of Contents

Product Focus

Mydoom Worm Scanner – The S4 MyDoom 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 the MyDoom email virus or its variants.

Check out our video section for a number of interviews with Jesper Jurcenoks:
www.netvigilance.com/videos

This Week in Review

A word n hackers and e-crime. E-crime congress in London in March. The power section constantly fight hackers. ID management.

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

- **Hackers Have Evolved, So Must Products**

The growing dependence on Web-based applications is simultaneously driving online commerce for SMEs, and criminal activities.

A couple of years ago hackers were mostly youngsters trying to spray paint their

name on big Web sites, but today we're dealing with serious, organised crime - these are professionals who are looking to make money by breaking into Web sites.

bios

Full Story :
http://www.biosmagazine.co.uk/op.php?id=800

❖ Stakeholders gear up for e-Crime Congress 2008

Over 500 delegates from global businesses, governments and law enforcement agencies will meet in London in March at the e-Crime Congress 2008 to discuss cyber-threats and electronic crime.

Identity theft and fraud continue to threaten security and consumer confidence, but last year saw an increasing number of attacks on the IT infrastructure of companies and governments.

This year's congress will focus on effective counter-measures against organised online crime, including electronic espionage, identity theft, data loss and online fraud.

vnunet

Full Story :
http://www.vnunet.com/vnunet/news/2207989/stakeholders-tackle-cyber-crime

❖ Hackers take aim at city power grids

Criminal hackers are increasingly targeting city power grids in an attempt to extort money from utility companies, the CIA has warned.

Security firms said that the warning from CIA senior analyst Tom Donahue came as no surprise.

"The assertion that hackers are breaking into power grid computer systems is not uncommon in this sector," said Geoff Sweeney, chief technology officer at security company Tier-3.

"The computerisation of power grids goes back to the 1980s and hackers, often working with inside knowledge of the computer systems, have been trying to down power systems ever since remote modems were hooked up to those systems."

vnunet

Full Story :
http://www.vnunet.com/vnunet/news/2207962/hackers-aim-city-power-grids

❖ Can't remember your password? Don't panic

Companies are competing to introduce a single, secure login that would work for all

bank accounts, shopping sites and other web activities
By her own admission, Anna Soames has no talent for remembering passwords.

Just to operate day-to-day, though, the London-based accountant needs no fewer than eight: three for work, another three for separate bank accounts, two for e-mail addresses she keeps, and one for her post-graduate university course. Each invariably has its own login.

“I generally go for a variation of my dog’s name,” Ms Soames, 29, said. “But sometimes that’s not long enough, so I have to add numbers after it, and then I forget which numbers, and so I end up writing them all down in the back of my diary – which kind of defeats the purpose, I guess.”

Timesonline

Full Story :
http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article1441331.ece

New Vulnerabilities Tested in SecureScout

- **16833 Oracle Application Server - Oracle Internet Directory component unspecified Vulnerability (jan-2008/AS06)**

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html

CVE Reference:

- **16832 Oracle Application Server - Oracle JDeveloper component unspecified Vulnerability (jan-2008/AS05)**

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html

CVE Reference:

- **16720 Oracle Application Server - Oracle Single Sign-On component unspecified Vulnerability (oct-2006/SSO02)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Single Sign-On component.

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

References:

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/449711/100/0/threaded
* CERT: TA06-291A
http://www.us-cert.gov/cas/techalerts/TA06-291A.html
* BID: 20588
http://www.securityfocus.com/bid/20588
* FRSIRT: ADV-2006-4065
http://www.frsirt.com/english/advisories/2006/4065
* SECTRACK: 1017077
http://securitytracker.com/id?1017077
* SECUNIA: 22396
http://secunia.com/advisories/22396

CVE Reference: CVE-2006-5363

- **16719 Oracle Application Server - Oracle Containers for J2EE component unspecified Vulnerability (oct-2006/OC4J04)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Containers for J2EE component.

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

References:

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-

updates/cpuoct2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/449711/100/0/threaded
* CERT: TA06-291A
http://www.us-cert.gov/cas/techalerts/TA06-291A.html
* BID: 20588
http://www.securityfocus.com/bid/20588
* FRSIRT: ADV-2006-4065
http://www.frsirt.com/english/advisories/2006/4065
* SECTRACK: 1017077
http://securitytracker.com/id?1017077
* SECUNIA: 22396
http://secunia.com/advisories/22396

CVE Reference: CVE-2006-5362

❖ 16718 Oracle Application Server - Oracle Containers for J2EE component unspecified Vulnerability (oct-2006/OC4J03)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Containers for J2EE component.

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

References:

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/449711/100/0/threaded
* CERT: TA06-291A
http://www.us-cert.gov/cas/techalerts/TA06-291A.html
* BID: 20588
http://www.securityfocus.com/bid/20588
* FRSIRT: ADV-2006-4065
http://www.frsirt.com/english/advisories/2006/4065
* SECTRACK: 1017077
http://securitytracker.com/id?1017077
* SECUNIA: 22396
http://secunia.com/advisories/22396

CVE Reference: CVE-2006-5361

❖ 16717 Oracle Application Server - Oracle Forms component unspecified Vulnerability (oct-2006/FORM03)

An unspecified vulnerability with unknown impact exists in Oracle Application Server

Oracle Forms component.

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

References:

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/449711/100/0/threaded
* CERT: TA06-291A
http://www.us-cert.gov/cas/techalerts/TA06-291A.html
* BID: 20588
http://www.securityfocus.com/bid/20588
* FRSIRT: ADV-2006-4065
http://www.frsirt.com/english/advisories/2006/4065
* SECTRACK: 1017077
http://securitytracker.com/id?1017077
* SECUNIA: 22396
http://secunia.com/advisories/22396

CVE Reference: CVE-2006-5360

❖ 16716 Oracle Application Server - Oracle Reports Developer component unspecified Vulnerability (oct-2006/REP02)

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

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

References:

* BUGTRAQ: 20061023 Various Cross-Site-Scripting Vulnerabilities in Oracle Reports
http://www.securityfocus.com/archive/1/archive/1/449503/100/0/threaded
* MISC:
http://www.red-database-security.com/advisory/oracle_reports_css.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/449711/100/0/threaded
* CERT: TA06-291A
http://www.us-cert.gov/cas/techalerts/TA06-291A.html
* BID: 20588
http://www.securityfocus.com/bid/20588
* FRSIRT: ADV-2006-4065
http://www.frsirt.com/english/advisories/2006/4065
* SECTRACK: 1017077

http://securitytracker.com/id?1017077
* SECUNIA: 22396
http://secunia.com/advisories/22396

CVE Reference: CVE-2006-5359

❖ 16715 Oracle Application Server - Oracle Reports Developer component unspecified Vulnerability (oct-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: **Medium**

References:

* BUGTRAQ: 20061023 Various Cross-Site-Scripting Vulnerabilities in Oracle Reports
http://www.securityfocus.com/archive/1/archive/1/449503/100/0/threaded
* MISC:
http://www.red-database-security.com/advisory/oracle_reports_css.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/449711/100/0/threaded
* CERT: TA06-291A
http://www.us-cert.gov/cas/techalerts/TA06-291A.html
* BID: 20588
http://www.securityfocus.com/bid/20588
* FRSIRT: ADV-2006-4065
http://www.frsirt.com/english/advisories/2006/4065
* SECTRACK: 1017077
http://securitytracker.com/id?1017077
* SECUNIA: 22396
http://secunia.com/advisories/22396

CVE Reference: CVE-2006-5359

❖ 16714 Oracle Application Server - Oracle HTTP Server component unspecified Vulnerability (oct-2006/OHS06)

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

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

References:

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/449711/100/0/threaded
* CERT: TA06-291A
http://www.us-cert.gov/cas/techalerts/TA06-291A.html
* BID: 20588
http://www.securityfocus.com/bid/20588
* FRSIRT: ADV-2006-4065
http://www.frsirt.com/english/advisories/2006/4065
* SECTRACK: 1017077
http://securitytracker.com/id?1017077
* SECUNIA: 22396
http://secunia.com/advisories/22396

CVE Reference: CVE-2006-5354

❖ 16713 Oracle Application Server - Oracle Containers for J2EE component unspecified Vulnerability (oct-2006/OC4J02)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Containers for J2EE component.

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

References:

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/449711/100/0/threaded
* CERT: TA06-291A
http://www.us-cert.gov/cas/techalerts/TA06-291A.html
* BID: 20588
http://www.securityfocus.com/bid/20588
* FRSIRT: ADV-2006-4065
http://www.frsirt.com/english/advisories/2006/4065
* SECTRACK: 1017077
http://securitytracker.com/id?1017077
* SECUNIA: 22396
http://secunia.com/advisories/22396

CVE Reference: CVE-2006-5356

New Vulnerabilities found this Week

Cisco PIX and ASA Time-To-Live Denial of Service Vulnerability

"Denial of Service"

Cisco has acknowledged a vulnerability in Cisco PIX and ASA appliances, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error in the processing of IP packets. This can be exploited to reload an affected device via specially crafted IP packets.

Successful exploitation requires that the Time-To-Live (TTL) decrement feature is enabled (disabled by default).

The vulnerability affects software versions 7.2(2) and later, prior to 7.2(3)006 or 8.0(3).

References:
http://www.cisco.com/warp/public/707/cisco-sa-20080123-asa.shtml

Microsoft Excel File Handling Code Execution

"code execution"

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

The vulnerability is caused due to an unspecified error in the handling of Excel files and can be exploited via a specially crafted Excel file with malformed header information.

Successful exploitation allows execution of arbitrary code but requires that the user is tricked into opening a malicious Excel file.

NOTE: According to Microsoft, this is currently being actively exploited.

The vulnerability is reported in the following versions:
* Microsoft Office Excel 2003 Service Pack 2
* Microsoft Office Excel Viewer 2003
* Microsoft Office Excel 2002
* Microsoft Office Excel 2000
* Microsoft Excel 2004 for Mac.

References:
http://www.microsoft.com/technet/security/advisory/947563.mspx

Winamp Ultravox Streaming Metadata Parsing Buffer Overflows

"execution of arbitrary code"

Secunia Research has discovered two vulnerabilities in Winamp, which can be exploited by malicious people to compromise a user's system.

The vulnerabilities are caused due to boundary errors in in_mp3.dll within the construction of stream titles when parsing Ultravox streaming metadata. This can be exploited to cause stack-based buffer overflows via overly long "<artist>" and "<name>" tag values in

the <metadata> section.

Successful exploitation allows execution of arbitrary code.

The vulnerabilities are confirmed in versions 5.21, 5.5, and 5.51. Other versions may also be affected.

References:
http://secunia.com/secunia_research/2008-2/

ISC BIND libbind "inet_network()" Off-By-One Vulnerability
"Denial of Service"

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

NOTE: The applications included in BIND 8 and 9 do not call the vulnerable function.

The vulnerability is reported in the following versions:
* BIND 8 (all versions)
* BIND 9.0 (all versions)
* BIND 9.1 (all versions)
* BIND 9.2 (all versions)
* BIND 9.3.0, 9.3.1, 9.3.2, 9.3.3, and 9.3.4
* BIND 9.4.0, 9.4.1, and 9.4.2
* BIND 9.5.0a1, 9.5.0a2, 9.5.0a3, 9.5.0a4, 9.5.0a5, 9.5.0a6, 9.5.0a7, and 9.5.0b1

References:
http://www.isc.org/index.pl?/sw/bind/bind-security.php

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