netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 29

July 18, 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.

This Week in Review

Virtual security requires teamwork. Unpatched machines under attack within 5 minutes.A look at the security risks with cloud computing.Business-like cybercriminals.

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

- **15 Jul 2008 13:00:00 Opinion: Good virtual security requires better IT teamwork**

July 15, 2008 (CIO) Virtualization security is not just about securing the virtual network, nor is it just about securing the virtualization server operating system.

Virtualization servers are a mix of a hypervisor device (OS), a networking device

(bridge or switch) and a storage interface.

Do you need a high-priced virtualization security expert to do this? These experts are few and far between, and you probably don"t need them. What you do need is the ability to pool all your security expertise in one group and educate them on the realities of virtualization. You need to remove the barriers and fiefdoms that spring up around IT and let these folks work together.

Computerworld

Full story:
http://feeds.computerworld.com/~r/Computerworld/Security/News/~3/336363125/article.do

- **14 Jul 2008 13:00:00 Unpatched Windows PCs fall to hackers in under 5 minutes, says ISC**

July 14, 2008 (Computerworld) It takes less than five minutes for hackers to find and compromise an unpatched Windows PC after it"s connected to the Internet, a security researcher said today.

"I have been asked many [times] by people if I really believed the survival time graph on the ISC site was truly an accurate representation of how long a new system had once connected," said Hutcheson. "The answer to this is "yes" for most home users and systems that are Internet-facing.

Another security researcher, however, said unpatched machines can last longer than just a few minutes before falling to attack. The German Honeypot Project, which sets vulnerable systems on the Internet to collect malware, estimates survival time in hours, not minutes.

Computerworld

Full story :
http://feeds.computerworld.com/~r/Computerworld/Security/News/~3/335295158/article.do

- **11 Jul 2008 13:00:00 The dangers of cloud computing**

July 11, 2008 (InfoWorld) The idea of cloud computing -- designed around an architecture whose natural state is a shared pool outside the enterprise -- has gained momentum in recent months as a way to reduce cost and improve IT flexibility. But the use of cloud computing also carries with it security risks, including perils related to compliance, availability, and data integrity.

"If you look around, go to any major facility, what is sitting in a box outside is an

alternative power supply. They don"t rely on just the grid," says Greenbaum. He argues that cloud computing should be no different.

Computerworld

Full story :
http://feeds.computerworld.com/~r/Computerworld/Security/News/~3/332820967/article.do

- **16 Jul 2008 13:39:33 Business booms for organized cybercriminals**

The days of the lone hacker are seemingly over, with cybercrime organizations now being run by bosses parading as business entrepreneurs, complete with criminal staff.

The findings, made by Finjan Software"s Malicious Code Research Center (MCRC), show that the "boss" does not commit crimes, rather leaves this to an "underboss" who provides trojans for attacks and also runs command and control functions".

Next in line are "campaign managers," who report to the so-called underboss and lead campaigns. They use their own affiliate networks as channels to perform attacks and steal data, which is then sold by individuals who are not directly involved in the attacks.

SC Magazine

Full story:

http://feeds.feedburner.com/~r/SCMagazineNews/~3/337273316/

New Vulnerabilities Tested in SecureScout

- **13645 Oracle Database Server - Advanced Queuing component unspecified Vulnerability (jul-2008/CVE-2008-2607)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Advanced Queuing" component.

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

References:

* CONFIRM:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

* SECUNIA: 31087

http://secunia.com/advisories/31087/

* IDEFENSE: Oracle Database DBMS_AQELM Package Buffer Overflow Vulnerability

http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=726

CVE Reference:

CVE-2008-2607 (cve.mitre.org, nvd.nist.gov)

- **13647 Oracle Database Server - Database Scheduler component unspecified Vulnerability (jul-2008/CVE-2008-2613)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Database Scheduler" component.

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

References:

* SECUNIA: 31087

http://secunia.com/advisories/31087/

* IDEFENSE: Oracle Database Local Untrusted Library Path Vulnerability

http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=727

* CONFIRM:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference:

CVE-2008-2613 (cve.mitre.org, nvd.nist.gov)

- **13648 Oracle Database Server - Advanced Replication component unspecified Vulnerability (jul-2008/CVE-2008-2592)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Advanced Replication" component.

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

References:

* SECUNIA: 31087

http://secunia.com/advisories/31087/

* CONFIRM:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference:

CVE-2008-2592 (cve.mitre.org, nvd.nist.gov)

- **13649 Oracle Database Server - Authentication component unspecified Vulnerability (jul-2008/CVE-2008-2604)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Authentication" component.

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

References:

* SECUNIA: 31087

http://secunia.com/advisories/31087/

* CONFIRM:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference:

CVE-2008-2604 (cve.mitre.org, nvd.nist.gov)

- **13650 Oracle Database Server - Oracle Database Vault component unspecified Vulnerability (jul-2008/CVE-2008-2591)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Oracle Database Vault" component.

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

References:

* SECUNIA: 31087

http://secunia.com/advisories/31087/

* CONFIRM:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference:

CVE-2008-2591 (cve.mitre.org, nvd.nist.gov)

- **13651 Oracle Database Server - Oracle Spatial component unspecified Vulnerability (jul-2008/CVE-2008-2600)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Oracle Spatial" component.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **Medium**

References:

* SECUNIA: 31087

http://secunia.com/advisories/31087/

* CONFIRM:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference:

CVE-2008-2600 (cve.mitre.org, nvd.nist.gov)

- **13652 Oracle Database Server - Data Pump component unspecified Vulnerability (jul-2008/CVE-2008-2602)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Data Pump" component.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **Medium**

References:

* SECUNIA: 31087

http://secunia.com/advisories/31087/

* CONFIRM:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference:

CVE-2008-2602 (cve.mitre.org, nvd.nist.gov)

- **13653 Oracle Database Server - Authentication component unspecified Vulnerability (jul-2008/CVE-2008-2605)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Authentication" component.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **Medium**

References:

* SECUNIA: 31087

http://secunia.com/advisories/31087/

* CONFIRM:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference:

CVE-2008-2605 (cve.mitre.org, nvd.nist.gov)

- **13654 Oracle Database Server - Core RDBMS component unspecified Vulnerability (jul-2008/CVE-2008-2611)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Core RDBMS" component.

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

References:

* SECUNIA: 31087

http://secunia.com/advisories/31087/

* CONFIRM:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference:

CVE-2008-2611 (cve.mitre.org, nvd.nist.gov)

- **13655 Oracle Database Server - Data Pump component unspecified Vulnerability (jul-2008/CVE-2008-2608)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Data Pump" component.

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

References:

* SECUNIA: 31087

http://secunia.com/advisories/31087/

* CONFIRM:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference:

CVE-2008-2608 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2008-3173 Microsoft CVSS 2.0 Score = 6.8**

Microsoft Internet Explorer allows web sites to set cookies for domains that have a public suffix with more than one dot character, which could allow remote attackers to perform a session fixation attack and hijack a user's HTTP session, aka "Cross-Site Cooking." NOTE: this issue may exist because of an insufficient fix for CVE-2004-0866.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

http://crisp.tweakblogs.net/blog/ie-and-2-letter-domain-names.html

http://kuza55.blogspot.com/2008/02/understanding-cookie-security.html

CVE Reference: CVE-2008-3173

- **CVE-2008-2597 Oracle CVSS 2.0 Score = 10.0**

Unspecified vulnerability in the TimesTen Client/Server component in Oracle Times Ten In-Memory Database 7.0.3.0.0 has unknown impact and remote attack vectors, a different vulnerability than CVE-2008-2598 and CVE-2008-2599.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference: CVE-2008-2597

- **CVE-2008-2611 Oracle CVSS 2.0 Score = 9.0**

Unspecified vulnerability in the Core RDBMS component in Oracle Database 9.0.1.5 FIPS+, 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.4, and 11.1.0.6 has unknown impact and remote authenticated attack vectors.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference: CVE-2008-2611

- **CVE-2008-2579 Oracle CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the WebLogic Server Plugins for Apache, Sun and IIS web servers component in BEA Product Suite 10.0 MP1, 9.2 MP3, 9.1, 9.0, 8.1 SP6, 7.0 SP7, and 6.1 SP7 has unknown impact and remote attack vectors.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference: CVE-2008-2579

- **CVE-2008-2580 Oracle CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.0 MP1, 9.2 MP3, 9.1, and 9.0 has unknown impact and remote attack vectors.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference: CVE-2008-2580

- **CVE-2008-2581 Oracle CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.0 MP1, 9.2 MP3, 9.1, 9.0, 8.1 SP6, and 7.0 SP7 has unknown impact and remote attack vectors related to UDDI Explorer.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference: CVE-2008-2581

- **CVE-2008-2582 Oracle CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.0 MP1, 9.2 MP3, 9.1, 9.0, 8.1 SP6, and 7.0 SP7 has unknown impact and remote attack vectors.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference: CVE-2008-2582

- **CVE-2008-2583 Oracle CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the sample Discussion Forum Portlet for the Oracle Portal component in Oracle Application Server, as available from OTN before 20080715, has unknown impact and remote attack vectors.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference: CVE-2008-2583

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