netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 1

January 4, 2008

Table of Contents

Product Focus

ASN.1 Vulnerability Scanner – The ASN.1 Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the MS04-007 that could allow remote code execution.

This Week in Review

Will hacker tools become unlawful? NHS and HIPAA on the same pace. Some good advice about being ready for the next threads. Researchers worry about city wi-fi's.

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

- **UK government to consider hacker tool ban**

The UK government has published guidelines for the application of a law that renders illegal the creation and distribution of 'hacking tools', The Register reports.
The law would increase the maximum jail term for hacking offences to 10 years and makes denial of service offences completely illegal.
The move to ban the development, ownership and distribution of hacker tools has received serious criticism from some in the industry.

CBR

Full Story :
http://www.cbronline.com/article_news.asp?guid=7DDE1F27-FAC8-4F61-9663-C148D6491C10

- **NHS & HIPAA: Drawing Parallels for Best Practices in Security & Patient Privacy**

The scope of the National Health Service (NHS) Connecting for Health program is immense – with a goal of moving toward an electronic care record (EHR) for every patient in the UK and to connect 30,000 general practitioners to more than 300 hospitals.

The program has battled lingering doubts about administrators' ability to manage patient security and confidentiality risks. Managing and controlling physician and workforce access to clinical and patient information is a significant challenge for a program of this magnitude. However, recent coverage of the security breach at North Tees Primary Care Trust, where multiple employees were able to review details of a celebrity's medical record, doesn't help instill confidence.

Public Technology

Full Story :
http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=13552

- **How to Prepare for Next Year's Security Threats**

With pundits making predictions for the state of cyber-crime and malicious software in 2008, one might be tempted to say, "OK, but what should I do with this information?" In some cases, this means an increase in specific types of attacks. In other cases, it means the rise of attacks against existing technologies. In all cases, it means that to prepare for next year's attacks you should keep doing what you already should have been doing this year, last year, and before that as well.

eweek

Full Story :
http://www.eweek.com/article2/0,1759,2243412,00.asp?kc=EWRSS03119TX1K0000594

- **Viruses to infect Wi-Fi networks in 2008?**

Researchers warn of potential for multi-network attack
Researchers at Indiana University have warned of the increased opportunity for hackers resulting from the spread of Wi-Fi. The researchers were specifically talking about the new breed of city-wide Wi-Fi networks where thousands can be logged on simultaneously, but the principle can also be applied to smaller-scale public hotspots.

What's more, the researchers think such a threat could piggyback across multiple Wi-Fi networks too, taking over thousands of networks in one fell swoop. The researchers think

such an attack would easily spread by guessing admin passwords that simply haven't been changed. In fact, they estimate that 36 per cent of passwords could be guessed.

Tech.co.uk

Full Story :
http://www.tech.co.uk/computing/networking-and-wi-fi/news/could-wi-fi-viruses-be-the-outlook-for-2008?articleid=565757107&source=rss

New Vulnerabilities Tested in SecureScout

- **16699 Oracle Application Server - Oracle Workflow Cartridge component unspecified Vulnerability (jan-2007/OWF01)**

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

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

References:

* BUGTRAQ: 20070117 [ISecAuditors Security Advisories] Oracle Reports Web Cartridge (RWCGI60) vulnerable to XSS
http://www.securityfocus.com/archive/1/archive/1/457193/100/0/threaded
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html
* CERT: TA07-017A
http://www.us-cert.gov/cas/techalerts/TA07-017A.html
* SECTRACK: 1017522
http://securitytracker.com/id?1017522
* SECUNIA: 23794
http://secunia.com/advisories/23794
* XF: oracle-cpu-jan2007(31541)
http://xforce.iss.net/xforce/xfdb/31541

CVE Reference: CVE-2007-0275

- **16698 Oracle Application Server - Oracle Containers for J2EE component unspecified Vulnerability (jan-2007/OC4J07)**

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:

* CONFIRM:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html
* CERT: TA07-017A
http://www.us-cert.gov/cas/techalerts/TA07-017A.html
* SECTRACK: 1017522
http://securitytracker.com/id?1017522
* SECUNIA: 23794
http://secunia.com/advisories/23794
* XF: oracle-cpu-jan2007(31541)
http://xforce.iss.net/xforce/xfdb/31541

CVE Reference: CVE-2007-0286

❖ 16697 Oracle Application Server - Oracle Process Mgmt & Notification component unspecified Vulnerability (jan-2007/OPMN02)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Process Mgmt & Notification component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html
* CERT: TA07-017A
http://www.us-cert.gov/cas/techalerts/TA07-017A.html
* SECTRACK: 1017522
http://securitytracker.com/id?1017522
* SECUNIA: 23794
http://secunia.com/advisories/23794
* XF: oracle-cpu-jan2007(31541)
http://xforce.iss.net/xforce/xfdb/31541

CVE Reference: CVE-2007-0282

❖ 16696 Oracle Application Server - Oracle Reports Developer component unspecified Vulnerability (jan-2007/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:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html
* CERT: TA07-017A
http://www.us-cert.gov/cas/techalerts/TA07-017A.html
* SECTRACK: 1017522
http://securitytracker.com/id?1017522
* SECUNIA: 23794
http://secunia.com/advisories/23794
* XF: oracle-cpu-jan2007(31541)
http://xforce.iss.net/xforce/xfdb/31541

CVE Reference: CVE-2007-0285

❖ 16695 Oracle Application Server - Oracle HTTP Server component unspecified Vulnerability (jan-2007/OHS04)

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:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html
* CERT: TA07-017A
http://www.us-cert.gov/cas/techalerts/TA07-017A.html
* SECTRACK: 1017522
http://securitytracker.com/id?1017522
* SECUNIA: 23794
http://secunia.com/advisories/23794
* XF: oracle-cpu-jan2007(31541)
http://xforce.iss.net/xforce/xfdb/31541

CVE Reference: CVE-2007-0281

❖ 16694 Oracle Application Server - Oracle HTTP Server component unspecified Vulnerability (jan-2007/OHS03)

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:

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

updates/cpujan2007.html
* CERT: TA07-017A
http://www.us-cert.gov/cas/techalerts/TA07-017A.html
* SECTRACK: 1017522
http://securitytracker.com/id?1017522
* SECUNIA: 23794
http://secunia.com/advisories/23794
* XF: oracle-cpu-jan2007(31541)
http://xforce.iss.net/xforce/xfdb/31541

CVE Reference: CVE-2007-0281

❖ 16693 Oracle Application Server - Oracle Containers for J2EE component unspecified Vulnerability (jan-2007/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: **Medium**

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html
* CERT: TA07-017A
http://www.us-cert.gov/cas/techalerts/TA07-017A.html
* SECTRACK: 1017522
http://securitytracker.com/id?1017522
* SECUNIA: 23794
http://secunia.com/advisories/23794
* XF: oracle-cpu-jan2007(31541)
http://xforce.iss.net/xforce/xfdb/31541

CVE Reference: CVE-2007-0284

❖ 16692 Oracle Application Server - Oracle Containers for J2EE component unspecified Vulnerability (jan-2007/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: **Medium**

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html
* CERT: TA07-017A
http://www.us-cert.gov/cas/techalerts/TA07-017A.html
* SECTRACK: 1017522

http://securitytracker.com/id?1017522
* SECUNIA: 23794
http://secunia.com/advisories/23794
* XF: oracle-cpu-jan2007(31541)
http://xforce.iss.net/xforce/xfdb/31541

CVE Reference: CVE-2007-0284

❖ 16691 Oracle Application Server - Oracle Containers for J2EE component unspecified Vulnerability (jan-2007/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:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html
* CERT: TA07-017A
http://www.us-cert.gov/cas/techalerts/TA07-017A.html
* SECTRACK: 1017522
http://securitytracker.com/id?1017522
* SECUNIA: 23794
http://secunia.com/advisories/23794
* XF: oracle-cpu-jan2007(31541)
http://xforce.iss.net/xforce/xfdb/31541

CVE Reference: CVE-2007-0283

❖ 16690 Oracle Application Server - Oracle Process Mgmt & Notification component unspecified Vulnerability (jan-2007/OPMN01)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Process Mgmt & Notification component.

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

References:

* MISC:
http://www.red-database-security.com/advisory/oracle_buffer_overflow_ons.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html
* CERT: TA07-017A
http://www.us-cert.gov/cas/techalerts/TA07-017A.html
* SECTRACK: 1017522

http://securitytracker.com/id?1017522
* SECUNIA: 23794
http://secunia.com/advisories/23794
* XF: oracle-cpu-jan2007(31541)
http://xforce.iss.net/xforce/xfdb/31541

CVE Reference: CVE-2007-0280

New Vulnerabilities found this Week

PHP Multiple Vulnerabilities

"bypass certain security restrictions"

Some vulnerabilities have been reported in PHP, where some have unknown impact and others can be exploited by malicious users to bypass certain security restrictions.

1) An integer overflow error exists in the "chunk_split()" function.

2) Integer overflow errors exists in the "strcspn()" and "strspn()" functions.

3) A regression error related to the "glob()" function exist, which can potentially be exploited to bypass the "open_basedir" directive.

4) An error exists within the handling of SQL queries containing "LOCAL INFILE" inside the MySQL extension. This can be exploited to bypass the "open_basedir" and "safe_mode" directives.

5) An error exists when processing "session_save_path" and "error_log" values, which can be exploited to bypass the "open_basedir" and "safe_mode" directives.

The vulnerabilities are reported in versions prior to 4.4.8.

References:
http://www.php.net/releases/4_4_8.php

RealPlayer Unspecified Buffer Overflow Vulnerability

"execution of arbitrary code"

Evgeny Legerov has reported a vulnerability in RealPlayer, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an unspecified error and can be exploited to cause a buffer overflow. No further information is available.

Successful exploitation allows execution of arbitrary code.

The vulnerability is reported in version 11 build 6.0.14.748. Other versions may also be affected.

References:

http://lists.immunitysec.com/pipermail/dailydave/2008-January/004811.html

Asterisk "BYE/Also" Denial of Service Vulnerability
"Denial of Service"

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

The vulnerability is caused due to a null-pointer dereference error within the handling of the "BYE/Also" transfer method and can be exploited to crash the application.

Successful exploitation requires that a dialog has already been established.

The vulnerability is reported in the following versions:
* Asterisk Open Source 1.4.x prior to version 1.4.17
* Asterisk Business Edition C.x.x prior to version C.1.0-beta8
* AsteriskNOW pre-release prior to beta7
* Asterisk Appliance Developer Kit prior to Asterisk 1.4 revision 95946
* s800i (Asterisk Appliance) 1.0.x prior to version 1.0.3.4

References:
http://downloads.digium.com/pub/security/AST-2008-001.html

Extended Module Player Multiple Buffer Overflow Vulnerabilities
"execution of arbitrary code"

Luigi Auriemma has discovered some vulnerabilities in Extended Module Player, which can be exploited by malicious people to compromise a vulnerable system.

1) A signedness error exists within the "test_oxm()" and "decrunch_oxm()" functions in misc/oxm.c. This can be exploited to cause a stack-based buffer overflow via a negative "ilen" field.

2) A boundary error within the "dtt_load()" function in loaders/dtt_load.c can be exploited to cause a stack-based buffer overflow via an overly large number of patterns (over 256).

Successful exploitation of the vulnerabilities allows execution of arbitrary code.

The vulnerabilities are confirmed in version 2.5.1. Other versions may also be affected.

References:
http://aluigi.altervista.org/adv/xmpbof-adv.txt

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