

## Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

---

## Product Focus

[WinArpd v1.0b8](#) - Download WinArpd executable by filling our download form. Size: 55KB

Download Here:

<http://www.netvigilance.com/productdownloads?productname=winarpd.exe.zip>

## This Week in Review

New lists from SANS and Mitre. Risk management in times of recession. Virtual machines directly on hardware more secure. Need for a better CAPTCHA.

Enjoy reading & Stay safe.

**Call or email netVigilance to get an update on SecureScout.**

**(503) 524 5758 or [sales@netVigilance.com](mailto:sales@netvigilance.com)**

## Top Security News Stories this Week

### • Frankly Speaking: What would really make software more secure

January 19, 2009 (Computerworld) Oh, not again. Last week, the SANS Institute and Mitre released yet another list of the most serious programming errors that break software security. And this time, SANS and Mitre got dozens of other organizations to sign on, including Microsoft, Apple, Oracle, Tata, Symantec, the Department of Homeland Security and the National Security Agency.

Yes, it's a fine list. It includes all our old favorites: overflowing buffers, unchecked input, random numbers that aren't really random, failure to block cross-site scripting and SQL injection. (You can find the complete list at [www.sans.org/top25errors](http://www.sans.org/top25errors).)

SANS and Mitre say this one is better, because this time they tapped dozens of other organizations to help compile the top 25 programming problems. Surely that will convince programmers to see the error of their ways and start coding securely, won't it?

Computerworld

Full Story :

### • Security Manager's Journal: Eyeing risks while cutting spending

January 19, 2009 (Computerworld) We're still dealing with fallout from the weakening economy. Besides the massive layoff I wrote about last time, each department has been told to decrease spending by 15%.

First up is intrusion detection. Our 12 sensors are positioned to monitor the DMZs at corporate and remote offices as well as major data centers and some interoffice communications. We're using several offshore analysts to monitor those sensors; they attend to the alerts and, when necessary, escalate things to our analysts here in the U.S. for evaluation and action. But we're definitely monitoring more attack signatures than we need to. Our analysts spend a good part of their days chasing false positives.

Action Plan: Do a thorough risk assessment before making any cuts. Risking a vulnerability in order to save money would be foolhardy -- and, in the long run, expensive.

Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=332097&source=rss> topic17

### • Virtual desktops getting security boost

January 22, 2009 (Network World) Businesses looking for safer virtual desktops can cut the risk of attacks if they run their virtual-machine hypervisors directly on computer hardware, eliminating reliance on separate operating systems that can be vulnerable to attack.

Beyond the security implications, client hypervisors offer the additional management benefits of centralizing content, enforcing access control to desktop images, updating and patching desktops and supporting multiple virtual machines on a single device while keeping them isolated from each other.

The Citrix client hypervisor is scheduled to be available around the time that VMware releases its client hypervisor. But the difference is that VMware's runs on top of the host machine's operating system, says Mark Bowker, an analyst with Enterprise Strategy Group.

Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9126671&source=rss> topic1

### • Building a better spam-blocking CAPTCHA

January 23, 2009 (Computerworld) How do you let people create user accounts or post comments on your Web site without letting spam bots in? Simple -- make your users prove they're human. Many Web sites use CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) technology to try to tell the bots from the people.

A basic CAPTCHA But while no one has yet come up with a computer that can fool people into thinking it's another person, computers are great at fooling other computers. These days, malware makers and spammers regularly trick the CAPTCHA systems at big-name Web sites such as Yahoo Mail, Gmail and Craigslist, and use these sites to automate their attacks.

Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9126378&source=rss> topic1

## New Vulnerabilities Tested in SecureScout

### • 13683 Oracle Database Server - Job Queue component unspecified Vulnerability (jan-2009/CVE-2008-5437)

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

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

References:

\* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>

\* SECUNIA: 33525

<http://secunia.com/advisories/33525/>

\* SECTRACK: 1021561: Oracle Database Lets Remote Authenticated Users Access and Modify Data and Cause Denial of Service Conditions

<http://securitytracker.com/alerts/2009/Jan/1021561.html>

\* MISC:

<http://blog.red-database-security.com/category/cpujan2009/>

**CVE Reference:**

CVE-2008-5437 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **13684 Oracle Database Server - Oracle OLAP component unspecified Vulnerability (jan-2009/CVE-2008-5436)**

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

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

**References:**

\* SECUNIA: 33525

<http://secunia.com/advisories/33525/>

\* SECTRACK: 1021561: Oracle Database Lets Remote Authenticated Users Access and Modify Data and Cause Denial of Service Conditions

<http://securitytracker.com/alerts/2009/Jan/1021561.html>

\* MISC:

<http://blog.red-database-security.com/category/cpujan2009/>

\* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>

**CVE Reference:**

CVE-2008-5436 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **13685 Oracle Database Server - Oracle Spatial component unspecified Vulnerability (jan-2009/CVE-2008-3978)**

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

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

**References:**

\* SECUNIA: 33525

<http://secunia.com/advisories/33525/>

\* SECTRACK: 1021561: Oracle Database Lets Remote Authenticated Users Access and Modify Data and Cause Denial of Service Conditions

<http://securitytracker.com/alerts/2009/Jan/1021561.html>

\* MISC:

<http://blog.red-database-security.com/category/cpujan2009/>

\* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>

**CVE Reference:**

CVE-2008-3978 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **13686 Oracle Database Server - Oracle Spatial component unspecified Vulnerability (jan-2009/CVE-2008-3979)**

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

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

**References:**

\* SECUNIA: 33525

<http://secunia.com/advisories/33525/>

\* SECTRACK: 1021561: Oracle Database Lets Remote Authenticated Users Access and Modify Data and Cause Denial of Service Conditions

<http://securitytracker.com/alerts/2009/Jan/1021561.html>

\* MISC:

<http://blog.red-database-security.com/category/cpujan2009/>

\* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>

**CVE Reference:**

CVE-2008-3979 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **13687 Oracle Database Server - Oracle Streams component unspecified Vulnerability (jan-2009/CVE-2008-4015)**

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

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

**References:**

\* SECUNIA: 33525

<http://secunia.com/advisories/33525/>

\* SECTRACK: 1021561: Oracle Database Lets Remote Authenticated Users Access and Modify Data and Cause Denial of Service Conditions

<http://securitytracker.com/alerts/2009/Jan/1021561.html>

\* MISC:

<http://blog.red-database-security.com/category/cpujan2009/>

\* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>

**CVE Reference:**

CVE-2008-4015 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **13688 Oracle Database Server - Oracle OLAP component unspecified Vulnerability (jan-2009/CVE-2008-3974)**

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

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

**References:**

\* SECUNIA: 33525

<http://secunia.com/advisories/33525/>

\* SECTRACK: 1021561: Oracle Database Lets Remote Authenticated Users Access and Modify Data and Cause Denial of Service Conditions

<http://securitytracker.com/alerts/2009/Jan/1021561.html>

\* MISC:

<http://blog.red-database-security.com/category/cpujan2009/>

\* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>

**CVE Reference:**

CVE-2008-3974 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **13689 Oracle Database Server - Oracle OLAP component unspecified Vulnerability (jan-2009/CVE-2008-3997)**

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

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

**References:**

\* SECUNIA: 33525

<http://secunia.com/advisories/33525/>

\* SECTRACK: 1021561: Oracle Database Lets Remote Authenticated Users Access and Modify Data and Cause Denial of Service Conditions

<http://securitytracker.com/alerts/2009/Jan/1021561.html>

\* MISC:

<http://blog.red-database-security.com/category/cpujan2009/>

\* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>

**CVE Reference:**

CVE-2008-3997 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **13690 Oracle Database Server - Oracle OLAP component unspecified Vulnerability (jan-2009/CVE-2008-3999)**

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

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

**References:**

\* SECUNIA: 33525

<http://secunia.com/advisories/33525/>

\* SECTRACK: 1021561: Oracle Database Lets Remote Authenticated Users Access and Modify Data and Cause Denial of Service Conditions

<http://securitytracker.com/alerts/2009/Jan/1021561.html>

\* MISC:

<http://blog.red-database-security.com/category/cpujan2009/>

\* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>

**CVE Reference:**

CVE-2008-3999 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **13691 Oracle Database Server - SQL\*Plus Windows GUI component unspecified Vulnerability (jan-2009/CVE-2008-5439)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "SQL\*Plus Windows GUI" component.

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

**References:**

\* SECUNIA: 33525

<http://secunia.com/advisories/33525/>

\* SECTRACK: 1021561: Oracle Database Lets Remote Authenticated Users Access and Modify Data and Cause Denial of Service Conditions

<http://securitytracker.com/alerts/2009/Jan/1021561.html>

\* MISC:

<http://blog.red-database-security.com/category/cpujan2009/>

\* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>

**CVE Reference:**

CVE-2008-5439 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **13692 Oracle Database Server - SQL\*Plus Windows GUI component unspecified Vulnerability (jan-2009/CVE-2008-3973)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "SQL\*Plus Windows GUI" component.

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

**References:**

\* SECUNIA: 33525

<http://secunia.com/advisories/33525/>

\* SECTRACK: 1021561: Oracle Database Lets Remote Authenticated Users Access and Modify Data and Cause Denial of Service Conditions

<http://securitytracker.com/alerts/2009/Jan/1021561.html>

\* MISC:

<http://blog.red-database-security.com/category/cpujan2009/>

\* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>

**CVE Reference:**

CVE-2008-3973 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## **New Vulnerabilities found this Week**

• **CVE-2008-5911 RealNetworks CVSS 2.0 Score = 10.0**

Multiple buffer overflows in RealNetworks Helix Server and Helix Mobile Server 11.x before 11.1.8 and 12.x before 12.0.1 allow remote attackers to (1) cause a denial of service via three crafted RTSP SETUP commands, or execute arbitrary code via (2) an NTLM authentication request with malformed base64-encoded data, (3) an RTSP DESCRIBE command, or (4) a DataConvertBuffer request.

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

**References:**

SECTRAK: <http://www.securitytracker.com/id?1021501>

SECTRAK: <http://www.securitytracker.com/id?1021500>

SECTRAK: <http://www.securitytracker.com/id?1021499>

SECTRAK: <http://www.securitytracker.com/id?1021498>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/3521>

SECUNIA: <http://secunia.com/advisories/33360>

CONFIRM: <http://docs.real.com/docs/security/SecurityUpdate121508HS.pdf>

**CVE Reference:** [CVE-2008-5911](#)

• **CVE-2008-2367 redhat CVSS 2.0 Score = 4.6**

Red Hat Certificate System 7.2 uses world-readable permissions for password.conf and unspecified other configuration files, which allows local users to discover passwords by reading these files.

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

**References:**

REDHAT: <https://rhn.redhat.com/errata/RHSA-2009-0006.html>

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=451998](https://bugzilla.redhat.com/show_bug.cgi?id=451998)

XF: <http://xforce.iss.net/xforce/xfdb/48021>

BID: <http://www.securityfocus.com/bid/33288>

SECTRAK: <http://securitytracker.com/id?1021608>

SECUNIA: <http://secunia.com/advisories/33540>

**CVE Reference:** [CVE-2008-2367](#)

• **CVE-2008-2368 redhat CVSS 2.0 Score = 4.6**

Red Hat Certificate System 7.2 stores passwords in cleartext in the UserDirEnrollment log, the RA wizard installer log, and unspecified other debug log files, and uses weak permissions for these files, which allows local users to discover passwords by reading the files.

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

**References:**

REDHAT: <https://rhn.redhat.com/errata/RHSA-2009-0006.html>

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=452000](https://bugzilla.redhat.com/show_bug.cgi?id=452000)

XF: <http://xforce.iss.net/xforce/xfdb/48022>

BID: <http://www.securityfocus.com/bid/33288>

SECTRAK: <http://securitytracker.com/id?1021608>

SECUNIA: <http://secunia.com/advisories/33540>

**CVE Reference:** [CVE-2008-2368](#)

## **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](mailto: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](mailto: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](mailto:info-scanner@securescout.net)