

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

[WinHoneyd v1.5c](#) - Download WinHoneyd executable package by filling our download form. Size: 2407KB

Download Here:

<http://www.netvigilance.com/productdownloads?productname=winhoneyd-1.5c.zip>

This Week in Review

ICANN calling for brainstorm on how to stop scams. P2P full of sensitive personal data. Think about what you really want everybody to know. Companies fear of laid-off workers.

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

• ICANN ponders ways to stop scammy Web sites

January 27, 2009 (IDG News Service) The overseer of the Internet's addressing system is soliciting ideas for how to fix a problem that is enabling spammers and fraudulent Web sites to flourish.

Fast flux allows an administrator to quickly point a domain name to a new IP address, for example, if the server at the first address fails or comes under a denial-of-service attack. It is legitimately used by content-distribution networks such as Akamai Technologies Inc. to balance loads, improve performance and lower data-transmission costs.

"Those engaged in these activities can frustrate the efforts of investigators to locate and shut down their operations by using fast-flux service networks to rapidly and continuously change the topology of the network on which their content is hosted," according to the report.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9126846&source=rss_topic1

• 12 tips for managing your information footprint

January 27, 2009 (Computerworld) When it comes to managing personal information online, most people are their own worst enemies. Many of us fail to adequately protect our personal data before it gets online, but once information makes its way to the Internet, it can be quickly replicated and is often difficult, if not impossible, to remove.

You can take an active role in managing data about you, whether it resides in marketing lists, government databases, telephone directories or credit reports. Here are some tips.

How much do you want to disclose about your employment history, likes and dislikes, and where you are at any given time? Do you really want everyone to know when you're not at home, how long you'll be out and when you'll be back?

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9125098&source=rss_topic1

• With economic slump, concerns rise over data theft

January 29, 2009 (IDG News Service) Is the worsening economic situation going to turn some employees into data thieves?

Crime rates spike during hard times, and with thousands of workers being laid off each week lately, there may be an added incentive for laid-off employees to take intellectual property with them to bolster their chances of getting hired with a competitor, to use with a start-up company of their own, or maybe even to sell.

According to Bromberger, companies that have their employee exit processes in order have less to fear from laid-off workers. It's just that with the current economic squeeze, people's motivation may be changing.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9126991&source=rss_topic1

• P2P networks rife with sensitive health care data, researcher warns

January 30, 2009 (Computerworld) Eric Johnson didn't have to break into a computer to gain access to a 1,718-page document containing Social Security numbers, dates of birth, insurance information, treatment codes and other health care data belonging to about 9,000 patients at a medical testing laboratory.

In all instances, Johnson was able to find and freely download the sensitive data from a peer-to-peer file-sharing network using some basic search terms.

The results of that study, which are scheduled to be published in the next few days, show that data leaks over P2P networks involving the health care sector pose a significant threat to patients, providers and payers, Johnson said.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127066&source=rss_topic1

New Vulnerabilities Tested in SecureScout

• 13675 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2008/CVE-2008-3983)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html>

* FRSIRT: ADV-2008-2825

<http://www.frsirt.com/english/advisories/2008/2825>

* SECTRAK: 1021050

<http://www.securitytracker.com/id?1021050>

* SECUNIA: 32291

<http://secunia.com/advisories/32291>

CVE Reference:

CVE-2008-3983 (cve.mitre.org, nvd.nist.gov)

• 13676 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2008/CVE-2008-3984)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html>

* FRSIRT: ADV-2008-2825

<http://www.frsirt.com/english/advisories/2008/2825>

* SECTRACK: 1021050

<http://www.securitytracker.com/id?1021050>

* SECUNIA: 32291

<http://secunia.com/advisories/32291>

CVE Reference:

CVE-2008-3984 (cve.mitre.org, nvd.nist.gov)

• 13677 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2008/CVE-2008-3994)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html>

* FRSIRT: ADV-2008-2825

<http://www.frsirt.com/english/advisories/2008/2825>

* SECTRACK: 1021050

<http://www.securitytracker.com/id?1021050>

* SECUNIA: 32291

<http://secunia.com/advisories/32291>

* XF: oracle-database-workspaceman-priv-escalation(45898)

<http://xforce.iss.net/xforce/xfdb/45898>

CVE Reference:

CVE-2008-3994 (cve.mitre.org, nvd.nist.gov)

• 13678 Oracle Database Server - Upgrade component unspecified Vulnerability (oct-2008/CVE-2008-3980)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html>

* FRSIRT: ADV-2008-2825

<http://www.frsirt.com/english/advisories/2008/2825>

* SECTRACK: 1021050

<http://www.securitytracker.com/id?1021050>

* SECUNIA: 32291

<http://secunia.com/advisories/32291>

CVE Reference:

CVE-2008-3980 (cve.mitre.org, nvd.nist.gov)

• 18256 Oracle Application Server - OC4J component unspecified Vulnerability (jan-2009/CVE-2008-4017)

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

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

References:

- * SECUNIA: 33525
<http://secunia.com/advisories/33525/>
- * SECTRACK: 1021572:Oracle Application Server Bugs Let Remote Users Access and Modify Data
<http://securitytracker.com/alerts/2009/Jan/1021572.html>
- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>
- * FRSIRT: ADV-2009-0115
<http://www.frsirt.com/english/advisories/2009/0115>
- * SECTRACK: 1021572
<http://www.securitytracker.com/id?1021572>

CVE Reference:

CVE-2008-4017 (cve.mitre.org, nvd.nist.gov)

• **18257 Oracle Application Server - Oracle BPEL Process Manager component unspecified Vulnerability (jan-2009/CVE-2008-4014)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Oracle BPEL Process Manager" component.

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

References:

- * SECUNIA: 33525
<http://secunia.com/advisories/33525/>
- * SECTRACK: 1021572:Oracle Application Server Bugs Let Remote Users Access and Modify Data
<http://securitytracker.com/alerts/2009/Jan/1021572.html>
- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>
- * FRSIRT: ADV-2009-0115
<http://www.frsirt.com/english/advisories/2009/0115>
- * SECTRACK: 1021572
<http://www.securitytracker.com/id?1021572>

CVE Reference:

CVE-2008-4014 (cve.mitre.org, nvd.nist.gov)

• **18258 Oracle Application Server - Oracle Portal component unspecified Vulnerability (jan-2009/CVE-2008-5438)**

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

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

References:

- * SECUNIA: 33525
<http://secunia.com/advisories/33525/>
- * SECTRACK: 1021572:Oracle Application Server Bugs Let Remote Users Access and Modify Data
<http://securitytracker.com/alerts/2009/Jan/1021572.html>
- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>
- * FRSIRT: ADV-2009-0115
<http://www.frsirt.com/english/advisories/2009/0115>
- * SECTRACK: 1021572
<http://www.securitytracker.com/id?1021572>

CVE Reference:

CVE-2008-5438 (cve.mitre.org, nvd.nist.gov)

• **18259 Oracle Application Server - Oracle JDeveloper component urability (jan-2009/CVE-2008-2623)**

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

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

References:

- * SECUNIA: 33525
<http://secunia.com/advisories/33525/>
- * SECTRACK: 1021572:Oracle Application Server Bugs Let Remote Users Access and Modify Data
<http://securitytracker.com/alerts/2009/Jan/1021572.html>
- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>
- * FRSIRT: ADV-2009-0115
<http://www.frsirt.com/english/advisories/2009/0115>
- * SECTRACK: 1021572
<http://www.securitytracker.com/id?1021572>

CVE Reference:

CVE-2008-2623 (cve.mitre.org, nvd.nist.gov)

• **18260 Oracle Enterprise Manager - Oracle Enterprise Manager component unspecified Vulnerability (jan-2009/CVE-2008-5447)**

An unspecified vulnerability with unknown impact exists in Oracle Enterprise Manager "Oracle Enterprise Manager" component.

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

References:

- * SECUNIA: 33525
<http://secunia.com/advisories/33525/>
- * SECTRACK: 1021569: Oracle Enterprise Manager Flaw Lets Remote Authenticated Users Access and Modify Data
<http://securitytracker.com/alerts/2009/Jan/1021569.html>
- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>
- * FRSIRT: ADV-2009-0115
<http://www.frsirt.com/english/advisories/2009/0115>
- * SECTRACK: 1021569
<http://www.securitytracker.com/id?1021569>

CVE Reference:

CVE-2008-5447 (cve.mitre.org, nvd.nist.gov)

• **18261 SMTP server detected**

A remote SMTP server has been detected. Some information disclosed by this server could be used to plan further attacks.

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

References:

CVE Reference:

New Vulnerabilities found this Week

• **CVE-2009-0320 Microsoft CVSS 2.0 Score = 4.0**

Microsoft Windows XP, Server 2003 and 2008, and Vista exposes I/O activity measurements of all processes, which allows local users to obtain sensitive information, as demonstrated by reading the I/O Other Bytes column in Task Manager (aka taskmgr.exe) to estimate the number of characters that a different user entered at a runas.exe password prompt, related to a "benchmarking attack."

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

References:

- BID: <http://www.securityfocus.com/bid/33440>
- BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/500393/100/0/threaded>

CVE Reference: [CVE-2009-0320](#)

• **CVE-2009-0277 Sun CVSS 2.0 Score = 7.8**

Unspecified vulnerability in the kernel in OpenSolaris snv_100 through snv_102 on the Sun UltraSPARC T2 and T2+ sun4v platforms allows local users to cause a denial of service (panic) via unknown vectors.

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

References:

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-66-250066-1>

XF: <http://xforce.iss.net/xforce/xfdb/48164>

BID: <http://www.securityfocus.com/bid/33398>

FRSIRT: <http://www.frst.com/english/advisories/2009/0209>

CVE Reference: [CVE-2009-0277](#)

• **CVE-2009-0304 Sun CVSS 2.0 Score = 7.8**

The kernel in Sun Solaris 10 and 11 snv_101b allows remote attackers to cause a denial of service (system crash) via a crafted IPv6 packet, as demonstrated by SunOSip6.c.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/48208>

BID: <http://www.securityfocus.com/bid/33435>

MILW0RM: <http://www.milw0rm.com/exploits/7865>

SECTRAK: <http://securitytracker.com/id?1021635>

SECUNIA: <http://secunia.com/advisories/33605>

FULLDISC: <http://lists.grok.org.uk/pipermail/full-disclosure/2009-January/067709.html>

CVE Reference: [CVE-2009-0304](#)

• **CVE-2009-0032 Apple CVSS 2.0 Score = 6.9**

CUPS on Mandriva Linux 2008.0, 2008.1, 2009.0, Corporate Server (CS) 3.0 and 4.0, and Multi Network Firewall (MNF) 2.0 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/pdf.log temporary file.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/48210>

BID: <http://www.securityfocus.com/bid/33418>

MANDRIVA: <http://www.mandriva.com/security/advisories?name=MDVSA-2009:029>

MANDRIVA: <http://www.mandriva.com/security/advisories?name=MDVSA-2009:028>

MANDRIVA: <http://www.mandriva.com/security/advisories?name=MDVSA-2009:027>

SECTRAK: <http://securitytracker.com/id?1021637>

CVE Reference: [CVE-2009-0032](#)

• **CVE-2009-0319 Sun CVSS 2.0 Score = 6.9**

Unspecified vulnerability in the autofs module in the kernel in Sun Solaris 8 through 10, and OpenSolaris before snv_108, allows local users to cause a denial of service (autofs mount outage) or possibly gain privileges via vectors related to "xdr processing problems."

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

References:

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-66-249966-1>

CONFIRM: <http://sunsolve.sun.com/search/document.do?assetkey=1-21-128624-09-1>

XF: <http://xforce.iss.net/xforce/xfdb/48234>

BID: <http://www.securityfocus.com/bid/33459>

FRSIRT: <http://www.frst.com/english/advisories/2009/0256>

CVE Reference: [CVE-2009-0319](#)

• **CVE-2009-0267 Sun CVSS 2.0 Score = 5.0**

libike in Sun Solaris 9 and 10, and OpenSolaris before snv_100, does not properly check packets, which allows remote attackers to cause a denial of service (in.iked daemon crash) via an unspecified IKE packet, a different vulnerability than CVE-2007-2989.

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

References:

BID: <http://www.securityfocus.com/bid/33407>

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-66-247406-1>

CONFIRM: <http://sunsolve.sun.com/search/document.do?assetkey=1-21-113451-15-1>

CVE Reference: [CVE-2009-0267](#)

• **CVE-2009-0278 Sun CVSS 2.0 Score = 5.0**

Sun Java System Application Server (AS) 8.1 and 8.2 allows remote attackers to read the Web Application configuration files in the (1) WEB-INF or (2) META-INF directory via a malformed request.

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

References:

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-66-245446-1>

CONFIRM: <http://sunsolve.sun.com/search/document.do?assetkey=1-21-119166-35-1>

XF: <http://xforce.iss.net/xforce/xfdb/48161>

BID: <http://www.securityfocus.com/bid/33397>

FRSIRT: <http://www.frst.com/english/advisories/2009/0208>

CVE Reference: [CVE-2009-0278](#)

• **CVE-2009-0268 Sun CVSS 2.0 Score = 4.9**

Race condition in the pseudo-terminal (aka pty) driver module in Sun Solaris 8 through 10, and OpenSolaris before snv_103, allows local users to cause a denial of service (panic) via unspecified vectors related to lack of "properly sequenced code" in ptc and ptsl.

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

References:

BID: <http://www.securityfocus.com/bid/33406>

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-66-249586-1>

CONFIRM: <http://sunsolve.sun.com/search/document.do?assetkey=1-21-113685-07-1>

XF: <http://xforce.iss.net/xforce/xfdb/48179>

CVE Reference: [CVE-2009-0268](#)

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