

## 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 v1.5b](#) - Download WinHoneyd executable package by filling our download form. Size: 2404KB

Download Here:

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

## This Week in Review

Costs of data breaches on the rise. Your browser and sll. Disk encryption and data recovery. Which browser to use - that is the question.

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

### • Costs of a Data Breach: Can You Afford \$6.65 Million?

February 4, 2009 (CIO) Affixing a dollar cost to a problem has immense benefit, and The Ponemon Institute goes to great lengths to arrive at the figures for its Annual Cost of a Data Breach Study.

In 2008 the average total cost of a data breach was \$6.65 million, up from \$6.35 million last year and \$4.54 in 2005. In 2008, the per-victim cost of a data breach was \$202, up from \$197 in 2007, and from \$138 when the study was launched in 2005. Breaches involving a third party to which data had been outsourced bore a per-victim cost of \$231, whereas self contained breaches bore a per-victim cost of \$179. Breaches that were the result of a malicious act bore a per-victim cost of \$225, whereas breaches that were the result of negligence bore a per-victim cost of \$199. Breaches that were the result of a lost or stolen laptop computer bore a per-victim cost of \$249, whereas breaches that did not involve a lost or stolen laptop computer bore a per-victim cost of \$177. If the data breach was a first-time event for the company the per victim cost was \$243, but if the company had experienced a breach previously the per victim cost was \$192.

Computerworld

Full Story :

### • Browser secrets of secure connections

February 3, 2009 (InfoWorld) Although most users don't know it, their Web browser plays a key part in determining the strength of the ciphers used between their client and an HTTPS-protected Web site. Encryption ciphers used in the SSL/TLS (Secure Sockets Layer/Transport Layer Security) negotiations can range from very strong to weak, and involve asymmetric ciphers, symmetric ciphers, key exchange algorithms and hash functions.

[ For more on browser security, see InfoWorld's special report, as well as individual reviews of Chrome, Firefox, Internet Explorer, Opera, and Safari. ]

Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127249&source=rss> topic1

### • New disk encryption standards could complicate data recovery

February 2, 2009 (Computerworld) When the world's largest disk-makers joined last week to announce a single standard for encrypting disk drives, the move raised questions among users about how to deal with full-disk encryption once it's native on all laptop or desktop computers.

"Then you have just killed yourself," said Dave Hill, an analyst at research firm Mesabi Group.

Some industry observers believe that within five years, all disk drive manufacturers will be offering drives -- both hard disk and solid-state disk -- that use the specifications for firmware-based encryption.

Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127178&source=rss> topic1

### • IE or Firefox: Which browser is more secure?

February 2, 2009 (CSO) The conventional wisdom in security circles used to be that Microsoft's Internet Explorer was hopelessly attack-prone and that only someone with a cyber death wish would prefer it over such alternatives as Mozilla Firefox, Opera or Apple's Safari browser.

CSOonline.com recently conducted a highly unscientific, very informal poll of security practitioners, asking which browser they consider more secure. Firefox still scores well for many who like the frequent and easy security updates. But IE seems to be gaining more acceptance, especially since Microsoft released version 7 a couple of years ago. As for Google's Chrome, the jury is still out.

Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127158&source=rss> topic1

## New Vulnerabilities Tested in SecureScout

### • 13679 Oracle Database Server - Oracle Application Express component unspecified Vulnerability (oct-2008/CVE-2008-4005)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Oracle Application Express" 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>

\* XF: oracle-database-apex-priv-escalation(45907)

<http://xforce.iss.net/xforce/xfdb/45907>

**CVE Reference:**

CVE-2008-4005 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **13680 Oracle Database Server - Core RDBMS component unspecified Vulnerability (oct-2008/CVE-2008-2625)**

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:**

\* BUGTRAQ: 20081019 CVE-2008-2625: Oracle DBMS ? Proxy Authentication Vulnerability  
<http://www.securityfocus.com/archive/1/archive/1/497539/100/0/threaded>

\* 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-db-coreldbms-unauth-access(45880)

<http://xforce.iss.net/xforce/xfdb/45880>

**CVE Reference:**

CVE-2008-2625 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **13681 Oracle Database Server - Oracle OLAP component unspecified Vulnerability (oct-2008/CVE-2008-3990)**

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:**

\* 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-2008-3990 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **13682 Oracle Database Server - Oracle OLAP component unspecified Vulnerability (oct-2008/CVE-2008-3991)**

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:**

\* 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-2008-3991 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **16678 Oracle Enterprise Manager - Database Control component unspecified Vulnerability (oct-2007/EM01)**

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

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

**References:**

- \* CONFIRM:  
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html>
- \* CERT: TA07-290A  
<http://www.us-cert.gov/cas/techalerts/TA07-290A.html>
- \* FRSIRT: ADV-2007-3524  
<http://www.frsirt.com/english/advisories/2007/3524>
- \* SECTRACK: 1018823  
<http://www.securitytracker.com/id?1018823>
- \* SECUNIA: 27251  
<http://secunia.com/advisories/27251>

**CVE Reference:**

CVE-2007-5530 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **16679 Oracle Enterprise Manager - Oracle Help for Web component unspecified Vulnerability (oct-2007/EM02)**

An unspecified vulnerability with unknown impact exists in Oracle Enterprise Manager Oracle Help for Web component.

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

**References:**

- \* CONFIRM:  
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html>
- \* CERT: TA07-290A  
<http://www.us-cert.gov/cas/techalerts/TA07-290A.html>
- \* FRSIRT: ADV-2007-3524  
<http://www.frsirt.com/english/advisories/2007/3524>
- \* SECTRACK: 1018823  
<http://www.securitytracker.com/id?1018823>
- \* SECUNIA: 27251  
<http://secunia.com/advisories/27251>

**CVE Reference:**

CVE-2007-5531 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **16686 Oracle Enterprise Manager - Oracle Agent component unspecified Vulnerability (apr-2007/EM01)**

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

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

**References:**

- \* MISC:  
[http://www.red-database-security.com/advisory/oracle\\_cpu\\_apr\\_2007.html](http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html)
- \* CONFIRM:  
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html>
- \* HP: HPSBMA02133  
<http://www.securityfocus.com/archive/1/archive/1/466329/100/200/threaded>
- \* BID: 23532  
<http://www.securityfocus.com/bid/23532>
- \* FRSIRT: ADV-2007-1426  
<http://www.frsirt.com/english/advisories/2007/1426>
- \* SECTRACK: 1017927  
<http://www.securitytracker.com/id?1017927>

**CVE Reference:**

CVE-2007-2129 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 16702 Oracle Enterprise Manager - Oracle Agent component unspecified Vulnerability (jan-2007/EM01)

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

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

#### 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-2007-0292 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 16703 Oracle Enterprise Manager - Oracle Agent component unspecified Vulnerability (jan-2007/EM02)

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

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

#### 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-2007-0292 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 16704 Oracle Enterprise Manager - Oracle Agent component unspecified Vulnerability (jan-2007/EM03)

An unspecified vulnerability with unknown impact exists in Oracle Enterprise Manager Oracle Agent 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-2007-0293 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

• **CVE-2009-0391 IBM CVSS 2.0 Score = 7.8**

Unspecified vulnerability in IBM WebSphere Application Server (WAS) 6.0.1 on z/OS allows attackers to read arbitrary files via unknown vectors.

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

**References:**

BID: <http://www.securityfocus.com/bid/33533>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PK79232>

SECUNIA: <http://secunia.com/advisories/33729>

**CVE Reference:** [CVE-2009-0391](#)

• **CVE-2009-0410 Novell CVSS 2.0 Score = 10.0**

Off-by-one error in the SMTP daemon in GroupWise Internet Agent (GWIA) in Novell GroupWise 6.5x, 7.0, 7.01, 7.02, 7.03, 7.03HP1a, and 8.0 allows remote attackers to execute arbitrary code via a long e-mail address in a malformed RCPT command, leading to a buffer overflow.

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

**References:**

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-09-010/>

CONFIRM: <http://download.novell.com/Download?buildid=GjZRRdqCFW0>

BID: <http://www.securityfocus.com/bid/33560>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/500609/100/0/threaded>

CONFIRM: <http://www.novell.com/support/viewContent.do?externalId=7002502>

SECUNIA: <http://secunia.com/advisories/33744>

**CVE Reference:** [CVE-2009-0410](#)

• **CVE-2009-0272 Novell CVSS 2.0 Score = 6.8**

Cross-site request forgery (CSRF) vulnerability in Novell GroupWise WebAccess 6.5x, 7.0, 7.01, 7.02x, 7.03, 7.03HP1a, and 8.0 allows remote attackers to insert e-mail forwarding rules, and modify unspecified other configuration settings, as arbitrary users via unknown vectors.

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

**References:**

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/500569/100/0/threaded>

MISC: [http://www.procheckup.com/vulnerability\\_manager/vulnerabilities/pr08-21](http://www.procheckup.com/vulnerability_manager/vulnerabilities/pr08-21)

CONFIRM: <http://www.novell.com/support/search.do?usemicrosite=true&searchString=7002319>

SECUNIA: <http://secunia.com/advisories/33744>

**CVE Reference:** [CVE-2009-0272](#)

• **CVE-2008-6024 Sun CVSS 2.0 Score = 5.4**

Unspecified vulnerability in the NFSv4 client module in the kernel on Sun Solaris 10 and OpenSolaris before snv\_37, when automountd is used, allows user-assisted remote attackers to cause a denial of service (unresponsive NFS filesystems) via unknown vectors.

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

**References:**

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-26-240546-1>

BID: <http://www.securityfocus.com/bid/30753>

**CVE Reference:** [CVE-2008-6024](#)

• **CVE-2009-0274 Novell CVSS 2.0 Score = 5.0**

Unspecified vulnerability in WebAccess in Novell GroupWise 6.5, 7.0, 7.01, 7.02x, 7.03, 7.03HP1a, and 8.0 might allow remote attackers to obtain sensitive information via a crafted URL, related to conversion of POST requests to GET requests.

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

**References:**

BID: <http://www.securityfocus.com/bid/33559>

CONFIRM: <http://www.novell.com/support/viewContent.do?externalId=7002322>

SECUNIA: <http://secunia.com/advisories/33744>

**CVE Reference:** [CVE-2009-0274](#)

• **CVE-2009-0273 Novell CVSS 2.0 Score = 4.3**

Multiple cross-site scripting (XSS) vulnerabilities in Novell GroupWise WebAccess 6.5x, 7.0, 7.01, 7.02x, 7.03, 7.03HP1a, and 8.0 allow remote attackers to inject arbitrary web script or HTML via the (1) User.id and (2) Library.queryText parameters to gw/webacc, and other vectors involving (3) HTML e-mail and (4) HTML attachments.

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

**References:**

BID: <http://www.securityfocus.com/bid/33541>

BID: <http://www.securityfocus.com/bid/33537>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/500575/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/500572/100/0/threaded>

MISC: [http://www.procheckup.com/vulnerability\\_manager/vulnerabilities/pr08-23](http://www.procheckup.com/vulnerability_manager/vulnerabilities/pr08-23)

MISC: [http://www.procheckup.com/vulnerability\\_manager/vulnerabilities/pr08-22](http://www.procheckup.com/vulnerability_manager/vulnerabilities/pr08-22)

CONFIRM: <http://www.novell.com/support/search.do?usemicrosite=true&searchString=7002321>

CONFIRM: <http://www.novell.com/support/search.do?usemicrosite=true&searchString=7002320>

SECUNIA: <http://secunia.com/advisories/33744>

**CVE Reference:** [CVE-2009-0273](#)

• **CVE-2009-0276 Google CVSS 2.0 Score = 5.0**

Cross-domain vulnerability in the V8 JavaScript engine in Google Chrome before 1.0.154.46 allows remote attackers to bypass the Same Origin Policy via a crafted script that accesses another frame and reads its full URL and possibly other sensitive information, or modifies the URL of this frame.

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

**References:**

CONFIRM: <http://src.chromium.org/viewvc/chrome?view=rev&revision=8524>

CONFIRM: <http://sites.google.com/a/chromium.org/dev/getting-involved/dev-channel/release-notes>

SECUNIA: <http://secunia.com/advisories/33754>

CONFIRM: <http://googlechromereleases.blogspot.com/2009/01/stable-beta-update-yahoo-mail-and.html>

CONFIRM: <http://codereview.chromium.org/18531>

**CVE Reference:** [CVE-2009-0276](#)

• **CVE-2009-0411 Google CVSS 2.0 Score = 5.0**

Google Chrome before 1.0.154.46 does not properly restrict access from web pages to the (1) Set-Cookie and (2) Set-Cookie2 HTTP response headers, which allows remote attackers to obtain sensitive information from cookies via XMLHttpRequest calls and other web script.

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

**References:**

CONFIRM: <http://src.chromium.org/viewvc/chrome?view=rev&revision=8529>

CONFIRM: <http://sites.google.com/a/chromium.org/dev/getting-involved/dev-channel/release-notes>

CONFIRM: <http://codereview.chromium.org/18533>

CONFIRM: <http://codereview.chromium.org/11264>

**CVE Reference:** [CVE-2009-0411](#)

**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)