

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

Much anticipated “Negev” released.

Our Web-interface for the Perimeter Service is now running dynamic pages based on “Ajax”, giving a much improved response time and customer experience. Existing customers can log right into the new system from the usual login page.

[RPC DCOM Vulnerabilities Scanner](#) – The Nimda Worm 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 MS IE Mime Header Flaw (MS01-020) or have been infected by the Nimda Worm.

CTO Jesper Jurcenoks of netVigilance is the keynote speaker at the ITEC Conference & Exhibition 2008 in Houston May 8, see <http://www.netvigilance.com/events>

This Week in Review

Hacking of websites seriously on the rise. More information from PCI. Data breeches a problem for more than 60% of UK businesses. Necessary security could make VoIP expensive.

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

❖ Hackers jack thousands of sites, including UN domains

Large numbers of legitimate websites, including government sites in the UK and some operated by the United Nations, have been hacked and are serving up malware, says a security researcher, as massive JavaScript attacks last detected in March resume.

"They're using the same techniques as last month, of an SQL injection of some sort," said Dan Hubbard, vice president of security research at Websense, referring to large-scale attacks that have plagued the internet since January.

Among the sites hacked, said Websense, were several affiliated with either the UN or UK government agencies.

computerworld

Full Story :

<http://computerworld.co.nz/news.nsf/scrt/F40D71621CD20AFDCC257435000DC19F>

❖ Two supplements to the PCI Data Security Standard

The PCI Security Standards Council announced the availability of two Information Supplements providing further clarification for PCI DSS requirement 11.3, regarding penetration testing, and Requirement 6.6, regarding application code review and application firewalls.

Both of these information supplements provide guidance to help merchants and service providers meet these two requirements in support of their PCI DSS compliance efforts. Both information supplements are now available on the Council's website.

helpnetsecurity

Full Story :

<http://www.net-security.org/secworld.php?id=6053>

❖ Infosec 08: Half of businesses hit by breaches

More than half of UK businesses have suffered at least one data breach during the last year, according to a survey released at Infosec 2008 in London.

According to an annual study by The Ponemon Institute and commissioned by PGP Corporation, 60 per cent of businesses suffered at least one data breach over the last 12 months. The results also showed 28 per cent of organisations had suffered two to five breaches.

Businesses were making more efforts to solve the problem with an increased uptake of data encryption. It showed that 15 per cent now had an encryption strategy applied consistently across the workplace, up from nine per cent in 2007.

itpro

Full Story :

<http://www.itpro.co.uk/news/191682/infosec-08-half-of-businesses-hit-by-breaches.html>

VoIP: When Cheaper Could Mean Costlier

It's no mystery why enterprises have fallen in love with VoIP. Long-distance calling for pennies on the dollar -- what's not to love? Unfortunately, security often takes a back seat to savings in VoIP implementation. Just like any other data, VoIP is hackable, and it could turn out to be costly.

For enterprises, the primary reason for adopting Voice over Internet Protocol (VoIP) phone service is money. Long-distance phone calls placed over the Internet typically cost a mere fraction of those placed under the business Over 800,000 High Quality Domains Available For Your Business. Click Here. rate plans offered by traditional telephone companies.

macnewsworld

Full Story :

<http://www.macnewsworld.com/story/must-read/62723.html>

New Vulnerabilities Tested in SecureScout

- **13629 Oracle Database Server - Data Pump component unspecified Vulnerability (apr-2008/DB11)**

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

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

References:

* SECUNIA: 29829

<http://secunia.com/advisories/29829/>

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html>

CVE Reference:

CVE-2008-1820 (cve.mitre.org, nvd.nist.gov)

• **13630 Oracle Database Server - Export component unspecified Vulnerability (apr-2008/DB12)**

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

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

References:

* SECUNIA: 29829

<http://secunia.com/advisories/29829/>

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html>

CVE Reference:

CVE-2008-1813 (cve.mitre.org, nvd.nist.gov)

• **13631 Oracle Database Server - Query Optimizer component unspecified Vulnerability (apr-2008/DB13)**

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

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

References:

* SECUNIA: 29829

<http://secunia.com/advisories/29829/>

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html>

* MISC:

http://www.red-database-security.com/advisory/oracle_outln_password_change.html

CVE Reference:

CVE-2008-1813 (cve.mitre.org, nvd.nist.gov)

- **13632 Oracle Database Server - Audit component unspecified Vulnerability (apr-2008/DB14)**

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

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

References:

* SECUNIA: 29829

<http://secunia.com/advisories/29829/>

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html>

CVE Reference:

CVE-2008-1816 (cve.mitre.org, nvd.nist.gov)

- **13633 Oracle Database Server - Advanced Queuing component unspecified Vulnerability (apr-2008/DB15)**

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

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

References:

* SECUNIA: 29829

<http://secunia.com/advisories/29829/>

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html>

CVE Reference:

CVE-2008-1821 (cve.mitre.org, nvd.nist.gov)

- **16750 Oracle Application Server - Oracle Reports Developer component unspecified Vulnerability (jan-2006/REP06)**

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:

* BUGTRAQ: 20060117 Oracle Reports - Overwrite any application server file via desname (fixed after 889 days)
<http://www.securityfocus.com/archive/1/archive/1/422257/30/7430/threaded>

* BUGTRAQ: 20060117 Oracle Reports - Read parts of files via desname (fixed after 874 days)
<http://www.securityfocus.com/archive/1/archive/1/422256/30/7430/threaded>

* MISC:
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html

* MISC:
http://www.red-database-security.com/advisory/oracle_reports_read_any_file.html

* CONFIRM:
<http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html>

* CERT-VN: VU#545804
<http://www.kb.cert.org/vuls/id/545804>

* BID: 16287
<http://www.securityfocus.com/bid/16287>

* FRSIRT: ADV-2006-0243
<http://www.frsirt.com/english/advisories/2006/0243>

* FRSIRT: ADV-2006-0323
<http://www.frsirt.com/english/advisories/2006/0323>

* SECTRAK: 1015499
<http://securitytracker.com/id?1015499>

* SECUNIA: 18493
<http://secunia.com/advisories/18493>

* SECUNIA: 18608
<http://secunia.com/advisories/18608>

* XF: oracle-january2006-update(24321)
<http://xforce.iss.net/xforce/xfdb/24321>

CVE Reference:

CVE-2006-0289 (cve.mitre.org, nvd.nist.gov)

• 16751 Oracle Application Server - Oracle Workflow Cartridge component unspecified Vulnerability (jan-2006/WF01)

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:

* CONFIRM:
<http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html>

* CERT-VN: VU#545804
<http://www.kb.cert.org/vuls/id/545804>

* BID: 16287
<http://www.securityfocus.com/bid/16287>

* FRSIRT: ADV-2006-0243
<http://www.frsirt.com/english/advisories/2006/0243>

* FRSIRT: ADV-2006-0323
<http://www.frsirt.com/english/advisories/2006/0323>
* SECTrack: 1015499
<http://securitytracker.com/id?1015499>
* SECUNIA: 18493
<http://secunia.com/advisories/18493>
* SECUNIA: 18608
<http://secunia.com/advisories/18608>
* XF: oracle-january2006-update(24321)
<http://xforce.iss.net/xforce/xfdb/24321>

CVE Reference:

CVE-2006-0290 (cve.mitre.org, nvd.nist.gov)

• 16913 Oracle Application Server - Oracle Jinitiator component unspecified Vulnerability (apr-2008/AS01)

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

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

References:

* CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html>
* SECTrack: 1019855
<http://www.securitytracker.com/id?1019855>
* SECUNIA: 29874
<http://secunia.com/advisories/29874>

CVE Reference:

CVE-2008-1823 (cve.mitre.org, nvd.nist.gov)

• 16914 Oracle Application Server - Oracle Dynamic Monitoring Service component unspecified Vulnerability (apr-2008/AS02)

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Oracle Dynamic Monitoring Service" component.

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

References:

* CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html>
* SECTrack: 1019855

<http://www.securitytracker.com/id?1019855>

* SECUNIA: 29874

<http://secunia.com/advisories/29874>

CVE Reference:

CVE-2008-1824 (cve.mitre.org, nvd.nist.gov)

• 16915 Oracle Application Server - Oracle Portal component unspecified Vulnerability (apr-2008/AS03)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html>

* SECTRAK: 1019855

<http://www.securitytracker.com/id?1019855>

* SECUNIA: 29874

<http://secunia.com/advisories/29874>

CVE Reference:

CVE-2008-1825 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

Adobe Products BMP Handling Buffer Overflow Vulnerability

"Execution of arbitrary code"

A vulnerability has been reported in multiple Adobe products, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error when handling BMP files. This can be exploited to cause a buffer overflow via a BMP file having a malformed header.

Successful exploitation may allow execution of arbitrary code via a specially crafted BMP file.

NOTE: Reportedly, the vulnerability can also be exploited when a malicious storage device (e.g. USB drives, cameras) is being attached to a vulnerable computer.

The vulnerability is reported in Adobe Photoshop Album Starter Edition 3.2 and Adobe After Effects CS3. Other versions may also be affected.

References:

<http://www.adobe.com/support/security/advisories/apsa08-04.html>

ICQ Personal Status Processing Buffer Overflow

“Execution of arbitrary code”

Leon Juranic has reported a vulnerability in ICQ, which can be exploited by malicious people to compromise another user's system.

The vulnerability is caused due to a boundary error when processing "Personal Statuses" set via the "Personal Status Manager" menu. This can be exploited to cause a heap-based buffer overflow by creating a specially crafted personal status and e.g. sending a message to another user.

Successful exploitation allows execution of arbitrary code.

The vulnerability is reported in version 6 build 6043. Other versions may also be affected.

References:

http://www.infigo.hr/en/in_focus/advisories/INFIGO-2008-04-08

Mozilla Firefox Javascript Garbage Collector Vulnerability

“Execution of arbitrary code”

A vulnerability has been reported in Mozilla Firefox, which can potentially be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error in the Javascript Garbage Collector and can be exploited to cause a memory corruption via specially crafted Javascript code.

Successful exploitation may allow execution of arbitrary code.

The vulnerability is reported in version 2.0.0.13. Prior versions may also be affected.

References:

<http://www.mozilla.org/security/announce/2008/mfsa2008-20.html>

Safari Multiple Vulnerabilities

“Execution of arbitrary code”

Some vulnerabilities have been reported in Safari, which can be exploited by malicious people to conduct cross-site scripting attacks or potentially to compromise a user's system.

1) An error exists in the handling of URLs containing a colon character in the host name. This can be exploited to conduct cross-site scripting attacks when a specially crafted URL is opened.

2) An integer overflow error exists in WebKit's regular expression compiler in JavaScriptCore/pcre/pcre_compile.cpp. This can be exploited to cause a heap-based buffer overflow via specially crafted regular expressions with large, nested repetition

counts.

Successful exploitation may allow execution of arbitrary code e.g. when a user visits a malicious web page.

The vulnerabilities are reported in versions prior to 3.1.1.

References:

<http://support.apple.com/kb/HT1467>

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@seurescout.net