

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

[Request Tracker for Windows \(WinRT\) by SecureScout Free Edition \(no upgrade\) v3.4.5 beta2](#) - Download Free WinRT v3.4.5 beta2 installer by filling our download form. Size: 34MB

Download Here:

http://www.netvigilance.com/productdownloads?productname=winrt_setup_3_4_5

This Week in Review

Companies fail to concentrate on greatest risks. New best practices for fighting botnets. Security considerations in the cloud. Compromised machines don't get cleaned.

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

• SANS finds pros overlooking dangers of client, web apps

Most organizations are stuck in the past, applying a disproportionate amount of focus on patching operating systems than on systems posing the greatest risk, according to a report released Tuesday by the SANS Institute.

Findings of the study, titled "Top Cyber Security Risks," were based on six months of data compiled this year by intrusion prevention provider TippingPoint and vulnerability management firm Qualys. The report found that most organizations are overlooking the parts of their networks most susceptible to attack: vulnerable client-side applications, such as Adobe Reader, Microsoft Office and Apple QuickTime, and internet facing websites. SC Magazine

Full Story :

<http://www.scmagazineus.com/SANS-finds-pros-overlooking-dangers-of-client-web-apps/article/148998/>

• Standard offers best practices for ISPs to fight botnets

The Internet Engineering Task Force (IETF) has published a draft standard calling for measures that internet service providers (ISPs) can use to defeat botnets.

The document says that mitigating botnet effects and remediating botnet systems could make it more difficult for networks of zombie computers to operate, in addition to reducing the level of online crime.

"Efforts by ISPs and other organizations could, over time, reduce the pool of computers infected with bots on the internet," the IETF draft said. SC Magazine

Full Story :

<http://www.scmagazineus.com/Standard-offers-best-practices-for-ISPs-to-fight-botnets/article/149162/>

• Security considerations critical in the cloud

With the dragging economy as a driver, IT departments are increasingly realizing the benefits of cloud security, but business leaders must ask themselves a few questions before handing over control to a third-party.

That was the message from analysts at a conference, "Gaining business and technical advantages from cloud, SaaS and hybrid security services," held Thursday in New York, and sponsored by consultancy IDC.

Cloud security is sometimes being driven - along with the cost saving benefits it provides - by what analysts referred to as "appliance fatigue," or the frustration of having to manage numerous on-premise security products. SC Magazine

Full Story :

<http://www.scmagazineus.com/Security-considerations-critical-in-the-cloud/article/149158/>

• Study: Malware persists on compromised machines

Eighty percent of computers that have been compromised are still infected after 30 days, and nearly 50 percent remain compromised after 10 months, according to an analysis released Wednesday by Trend Micro.

"When machines are compromised, they're compromised for a long time," Dave Rand, CTO of Trend Micro, told SCMagazineUS.com Wednesday.

The machines remain undiscovered because they tend to stay under the radar - they don't do anything blatant, such as consuming system resources, that would tip off the victim, he said. SC Magazine

Full Story :

<http://www.scmagazineus.com/Study-Malware-persists-on-compromised-machines/article/149089/>

New Vulnerabilities Tested in SecureScout

• 18511 QuickTime handling of H.264 movie files, memory corruption issue (Remote File Checking)

A memory corruption issue exists in QuickTime's handling of H.264 movie files. Viewing a maliciously crafted H.264 movie file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.6.4.

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

References:

* CONFIRM:

<http://support.apple.com/kb/HT3859>

* APPLE: APPLE-SA-2009-09-09-2

<http://lists.apple.com/archives/security-announce/2009/Sep/msg00002.html>

* BID: 36328

<http://www.securityfocus.com/bid/36328>

CVE Reference:

CVE-2009-2202 (cve.mitre.org, nvd.nist.gov)

• 18512 QuickTime handling of MPEG-4 video files, buffer overflow vulnerability (Remote File Checking)

A buffer overflow exists in QuickTime's handling of MPEG-4 video files. Opening a maliciously crafted MPEG-4 video file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.6.4.

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

References:

- * CONFIRM:
<http://support.apple.com/kb/HT3859>
- * APPLE: APPLE-SA-2009-09-09-2
<http://lists.apple.com/archives/security-announce/2009/Sep/msg00002.html>
- * BID: 36328
<http://www.securityfocus.com/bid/36328>

CVE Reference:

CVE-2009-2203 (cve.mitre.org, nvd.nist.gov)

• 18513 QuickTime handling of FlashPix files, heap buffer overflow vulnerability (Remote File Checking)

A heap buffer overflow exists in QuickTime's handling of FlashPix files. Viewing a maliciously crafted FlashPix file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.6.4.

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

References:

- * CONFIRM:
<http://support.apple.com/kb/HT3859>
- * APPLE: APPLE-SA-2009-09-09-2
<http://lists.apple.com/archives/security-announce/2009/Sep/msg00002.html>
- * BID: 36328
<http://www.securityfocus.com/bid/36328>

CVE Reference:

CVE-2009-2798 (cve.mitre.org, nvd.nist.gov)

• 18514 QuickTime handling of H.264 movie files, heap buffer overflow vulnerability (Remote File Checking)

A heap buffer overflow exists in QuickTime's handling of H.264 movie files. Viewing a maliciously crafted H.264 movie file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.6.4.

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

References:

- * CONFIRM:
<http://support.apple.com/kb/HT3859>
- * APPLE: APPLE-SA-2009-09-09-2
<http://lists.apple.com/archives/security-announce/2009/Sep/msg00002.html>
- * BID: 36328
<http://www.securityfocus.com/bid/36328>

CVE Reference:

CVE-2009-2799 (cve.mitre.org, nvd.nist.gov)

• 18515 PHP Array index error in imageRotate function, information disclosure Vulnerability

Array index error in the imageRotate function in PHP 5.2.8 and earlier allows context-dependent attackers to read the contents of arbitrary memory locations via a crafted value of the third argument (aka the bgd_color or clrBack argument) for an indexed image.

The issue has been fixed in PHP versions 5.2.9.

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

References:

- * MISC:
<http://downloads.securityfocus.com/vulnerabilities/exploits/33002-2.php>
- * MISC:
<http://downloads.securityfocus.com/vulnerabilities/exploits/33002.php>
- * CONFIRM:

http://cvs.php.net/viewvc.cgi/php-src/NEWS?r1=1.2027.2.547.2.1360&r2=1.2027.2.547.2.1361&diff_format=u

* CONFIRM:

http://www.php.net/releases/5_2_9.php

* CONFIRM:

<http://support.apple.com/kb/HT3865>

* APPLE: APPLE-SA-2009-09-10-2

<http://lists.apple.com/archives/security-announce/2009/Sep/msg00004.html>

* FEDORA: FEDORA-2009-3768

<https://www.redhat.com/archives/fedora-package-announce/2009-May/msg01451.html>

* FEDORA: FEDORA-2009-3848

<https://www.redhat.com/archives/fedora-package-announce/2009-May/msg01465.html>

* HP: HPSBUX02431

<http://marc.info/?l=bugtraq&m=124654546101607&w=2>

* MANDRIVA: MDVSA-2009:021

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:021>

* MANDRIVA: MDVSA-2009:022

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:022>

* MANDRIVA: MDVSA-2009:023

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:023>

* REDHAT: RHSA-2009:0350

<http://www.redhat.com/support/errata/RHSA-2009-0350.html>

* SUSE: SUSE-SR:2009:008

<http://lists.opensuse.org/opensuse-security-announce/2009-04/msg00003.html>

* BID: 33002

<http://www.securityfocus.com/bid/33002>

* OSVDB: 51031

<http://osvdb.org/51031>

* SECTrack: 1021494

<http://securitytracker.com/id?1021494>

* SECUNIA: 34642

<http://secunia.com/advisories/34642>

* SECUNIA: 35306

<http://secunia.com/advisories/35306>

* SECUNIA: 35650

<http://secunia.com/advisories/35650>

* SECUNIA: 36701

<http://secunia.com/advisories/36701>

* XF: php-imagerotate-info-disclosure(47635)

<http://xforce.iss.net/xforce/xfdb/47635>

CVE Reference:

CVE-2008-5498 (cve.mitre.org, nvd.nist.gov)

• 18516 PHP JSON_parser function, Denial of Service Vulnerability

The JSON_parser function (ext/json/JSON_parser.c) in PHP 5.2.x before 5.2.9 allows remote attackers to cause a denial of service (segmentation fault) via a malformed string to the json_decode API function.

The issue has been fixed in PHP versions 5.2.9.

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

References:

* MLIST: [oss-security] 20090401 CVE request: PHP 5.2.9

<http://www.openwall.com/lists/oss-security/2009/04/01/9>

* MISC:

http://cvs.php.net/viewvc.cgi/php-src/ext/json/JSON_parser.c?r1=1.1.2.14&r2=1.1.2.15

* CONFIRM:

http://www.php.net/releases/5_2_9.php

* CONFIRM:

<http://support.apple.com/kb/HT3865>

* APPLE: APPLE-SA-2009-09-10-2

<http://lists.apple.com/archives/security-announce/2009/Sep/msg00004.html>

* DEBIAN: DSA-1775

<http://www.debian.org/security/2009/dsa-1775>

* DEBIAN: DSA-1789

<http://www.debian.org/security/2009/dsa-1789>

* FEDORA: FEDORA-2009-3768

<https://www.redhat.com/archives/fedora-package-announce/2009-May/msg01451.html>

* FEDORA: FEDORA-2009-3848
<https://www.redhat.com/archives/fedora-package-announce/2009-May/msg01465.html>
* MANDRIVA: MDVSA-2009:090
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:090>
* REDHAT: RHSA-2009:0350
<http://www.redhat.com/support/errata/RHSA-2009-0350.html>
* SUSE: SUSE-SR:2009:012
<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>
* UBUNTU: USN-761-1
<http://www.ubuntu.com/support/documentation/usn/usn-761-1>
* UBUNTU: USN-761-2
<http://www.ubuntu.com/usn/USN-761-2>
* SECUNIA: 34770
<http://secunia.com/advisories/34770>
* SECUNIA: 34830
<http://secunia.com/advisories/34830>
* SECUNIA: 34933
<http://secunia.com/advisories/34933>
* SECUNIA: 35003
<http://secunia.com/advisories/35003>
* SECUNIA: 35007
<http://secunia.com/advisories/35007>
* SECUNIA: 35306
<http://secunia.com/advisories/35306>
* SECUNIA: 35685
<http://secunia.com/advisories/35685>
* SECUNIA: 36701
<http://secunia.com/advisories/36701>
* BID: 33927
<http://www.securityfocus.com/bid/33927>

CVE Reference:

CVE-2009-1271 (cve.mitre.org, nvd.nist.gov)

• 18517 PHP `php_zip_make_relative_path` function, Denial of Service Vulnerability

The `php_zip_make_relative_path` function in `php_zip.c` in PHP 5.2.x before 5.2.9 allows context-dependent attackers to cause a denial of service (crash) via a ZIP file that contains filenames with relative paths, which is not properly handled during extraction.

The issue has been fixed in PHP versions 5.2.9.

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

References:

* BID: 33927
<http://www.securityfocus.com/bid/33927>
* MLIST: [oss-security] 20090401 CVE request: PHP 5.2.9
<http://www.openwall.com/lists/oss-security/2009/04/01/9>
* MLIST: [oss-security] 20090409 Re: CVE request: PHP 5.2.9
<http://www.openwall.com/lists/oss-security/2009/04/09/1>
* MISC:
http://cvs.php.net/viewvc.cgi/php-src/ext/zip/php_zip.c?r1=1.1.2.48&r2=1.1.2.49
* CONFIRM:
http://www.php.net/releases/5_2_9.php
* CONFIRM:
<http://support.apple.com/kb/HT3865>
* APPLE: APPLE-SA-2009-09-10-2
<http://lists.apple.com/archives/security-announce/2009/Sep/msg00004.html>
* HP: HPSBMA02447
<http://marc.info/?l=bugtraq&m=125017764422557&w=2>
* SUSE: SUSE-SR:2009:012
<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>
* SECUNIA: 35685
<http://secunia.com/advisories/35685>
* SECUNIA: 36701
<http://secunia.com/advisories/36701>

CVE Reference:

CVE-2009-1272 (cve.mitre.org, nvd.nist.gov)

• 18518 PHP exif_read_data function, Denial of Service Vulnerability

The exif_read_data function in the Exif module in PHP before 5.2.10 allows remote attackers to cause a denial of service (crash) via a malformed JPEG image with invalid offset fields, a different issue than CVE-2005-3353.

The issue has been fixed in PHP versions 5.2.10.

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

References:

- * CONFIRM:
<http://bugs.php.net/bug.php?id=48378>
- * CONFIRM:
http://www.php.net/releases/5_2_10.php
- * MANDRIVA: MDVSA-2009:167
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:167>
- * MANDRIVA: MDVSA-2009:145
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:145>
- * UBUNTU: USN-824-1
<http://www.ubuntulinux.org/support/documentation/usn/usn-824-1>
- * BID: 35440
<http://www.securityfocus.com/bid/35440>
- * OSVDB: 55222
<http://osvdb.org/55222>
- * SECUNIA: 35441
<http://secunia.com/advisories/35441>
- * SECUNIA: 36462
<http://secunia.com/advisories/36462>
- * VUPEN: ADV-2009-1632
<http://www.vupen.com/english/advisories/2009/1632>
- * XF: php-exifreaddata-dos(51253)
<http://xforce.iss.net/xforce/xfdb/51253>

CVE Reference:

CVE-2009-2687 (cve.mitre.org, nvd.nist.gov)

• 18519 PHP OpenSSL ASN1 printing crash Vulnerability

PHP is vulnerable to the following issue because it includes a vulnerable version of the OpenSSL library.

The function ASN1_STRING_print_ex() when used to print a BMPString or UniversalString will crash with an invalid memory access if the encoded length of the string is illegal. (CVE-2009-0590)

Any OpenSSL application which prints out the contents of a certificate could be affected by this bug, including SSL servers, clients and S/MIME software.

PHP 5.2.9 fixes the issue.

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

References:

- * CONFIRM:
http://sourceforge.net/project/shownotes.php?release_id=671059&group_id=116847
- * CONFIRM:
<http://voodoo-circle.sourceforge.net/sa/sa-20090326-01.html>
- * CONFIRM: secadv_20090325
http://www.openssl.org/news/secadv_20090325.txt
- * CONFIRM:
<http://www.php.net/archive/2009.php#id2009-04-08-1>
- * DEBIAN: DSA-1763
<http://www.debian.org/security/2009/dsa-1763>
- * MANDRIVA: MDVSA-2009:087
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:087>
- * UBUNTU: USN-750-1
<http://www.ubuntu.com/usn/usn-750-1>
- * BID: 34256
<http://www.securityfocus.com/bid/34256>
- * OSVDB: 52864

<http://www.osvdb.org/52864>

* SECTrack: 1021905

<http://securitytracker.com/id?1021905>

* SECUNIA: 34411

<http://secunia.com/advisories/34411>

* SECUNIA: 34460

<http://secunia.com/advisories/34460>

* SECUNIA: 34509

<http://secunia.com/advisories/34509>

* SECUNIA: 34666

<http://secunia.com/advisories/34666>

* VUPEN: ADV-2009-0850

<http://www.vupen.com/english/advisories/2009/0850>

* XF: openssl-asn1-stringprintex-dos(49431)

<http://xforce.iss.net/xforce/xfdb/49431>

CVE Reference:

CVE-2009-0590 (cve.mitre.org, nvd.nist.gov)

• 18520 PHP OpenSSL Incorrect Error Checking During CMS verification Vulnerability

PHP is vulnerable to the following issue because it includes a vulnerable version of the OpenSSL library.

The function CMS_verify() does not correctly handle an error condition involving malformed signed attributes. This will cause an invalid set of signed attributes to appear valid and content digests will not be checked.

These malformed attributes cannot be generated without access to the signer's private key so an attacker cannot forge signatures. A valid signer could however generate an invalid signature which appears valid and later repudiate the signature.

The older PKCS#7 code is not affected.

This issue only affects CMS users: CMS is only present in OpenSSL 0.9.8h and later where it is disabled by default and 0.9.9-dev.

PHP 5.2.9 fixes the issue.

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

References:

* CONFIRM:

http://sourceforge.net/project/shownotes.php?release_id=671059&group_id=116847

* CONFIRM:

<http://voodoo-circle.sourceforge.net/sa/sa-20090326-01.html>

* CONFIRM: secadv_20090325

http://www.openssl.org/news/secadv_20090325.txt

* CONFIRM:

<http://www.php.net/archive/2009.php#id2009-04-08-1>

* BID: 34256

<http://www.securityfocus.com/bid/34256>

* OSVDB: 52865

<http://www.osvdb.org/52865>

* SECTrack: 1021907

<http://securitytracker.com/id?1021907>

* SECUNIA: 34411

<http://secunia.com/advisories/34411>

* SECUNIA: 34460

<http://secunia.com/advisories/34460>

* SECUNIA: 34666

<http://secunia.com/advisories/34666>

* VUPEN: ADV-2009-0850

<http://www.vupen.com/english/advisories/2009/0850>

* XF: openssl-cmsverify-security-bypass(49432)

<http://xforce.iss.net/xforce/xfdb/49432>

CVE Reference:

CVE-2009-0591 (cve.mitre.org, nvd.nist.gov)

• 18521 PHP OpenSSL Invalid ASN1 clearing check Vulnerability

PHP is vulnerable to the following issue because it includes a vulnerable version of the OpenSSL library.

When a malformed ASN1 structure is received it's contents are freed up and zeroed and an error condition returned. On a small number of platforms where `sizeof(long) < sizeof(void *)` (for example WIN64) this can cause an invalid memory access later resulting in a crash when some invalid structures are read, for example RSA public keys (CVE-2009-0789).

Any OpenSSL application which uses the public key of an untrusted certificate could be crashed by a malformed structure. Including SSL servers, clients, CA and S/MIME software.

Users of OpenSSL 0.9.8 on affected platforms should update to 0.9.8k which contains a patch to correct this issue.

Thanks to Paolo Ganci for reporting this issue.

PHP 5.2.9 fixes the issue.

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

References:

- * CONFIRM:
http://sourceforge.net/project/shownotes.php?release_id=671059&group_id=116847
- * CONFIRM:
<http://voodoo-circle.sourceforge.net/sa/sa-20090326-01.html>
- * CONFIRM: secadv_20090325
http://www.openssl.org/news/secadv_20090325.txt
- * CONFIRM:
<http://www.php.net/archive/2009.php#id2009-04-08-1>
- * BID: 34256
<http://www.securityfocus.com/bid/34256>
- * OSVDB: 52866
<http://www.osvdb.org/52866>
- * SECTRACK: 1021906
<http://securitytracker.com/id?1021906>
- * SECUNIA: 34411
<http://secunia.com/advisories/34411>
- * SECUNIA: 34460
<http://secunia.com/advisories/34460>
- * SECUNIA: 34666
<http://secunia.com/advisories/34666>
- * VUPEN: ADV-2009-0850
<http://www.vupen.com/english/advisories/2009/0850>
- * XF: openssl-asn1-structure-dos(49433)
<http://xforce.iss.net/xforce/xfdb/49433>

CVE Reference:

CVE-2009-0789 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-7217 Microsoft CVSS 2.0 Score = 4.6

Microsoft Office 2008 for Mac, when running on Macintosh systems that restrict Office access to administrators, does not enforce this restriction for user ID 502, which allows local users with that ID to bypass intended security policy and access Office programs, related to permissions and ownership for certain directories.

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

References:

MSKB: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;948488>

OSVDB: <http://osvdb.org/44959>

CVE Reference: [CVE-2008-7217](http://cve.mitre.org/cve/2008/7217)

• CVE-2008-7233 Oracle CVSS 2.0 Score = 9.3

Unspecified vulnerability in the E-Business Application client, as used in Oracle Application Server 1.1.8.26 and E-Business Suite 11.5.10.2, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to the Oracle Jinitiator component, aka AS02.

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

References:

CERT: <http://www.us-cert.gov/cas/techalerts/TA08-017A.html>

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html>

VUPEN: <http://www.vupen.com/english/advisories/2008/0180>

VUPEN: <http://www.vupen.com/english/advisories/2008/0150>

BID: <http://www.securityfocus.com/bid/27229>

OSVDB: <http://www.osvdb.org/40294>

SECTRAK: <http://securitytracker.com/id?1019218>

SECUNIA: <http://secunia.com/advisories/28556>

SECUNIA: <http://secunia.com/advisories/28518>

HP: <http://marc.info/?l=bugtraq&m=120058413923005&w=2>

HP: <http://marc.info/?l=bugtraq&m=120058413923005&w=2>

CVE Reference: [CVE-2008-7233](#)

• **CVE-2008-7234 Oracle CVSS 2.0 Score = 6.8**

Unspecified vulnerability in the Oracle BPEL Worklist Application component in Oracle Application Server 10.1.2.2 and 10.1.3.3 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors, aka AS03.

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

References:

CERT: <http://www.us-cert.gov/cas/techalerts/TA08-017A.html>

VUPEN: <http://www.vupen.com/english/advisories/2008/0180>

VUPEN: <http://www.vupen.com/english/advisories/2008/0150>

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html>

SECTRAK: <http://securitytracker.com/id?1019218>

HP: <http://marc.info/?l=bugtraq&m=120058413923005&w=2>

HP: <http://marc.info/?l=bugtraq&m=120058413923005&w=2>

BID: <http://www.securityfocus.com/bid/27229>

OSVDB: <http://www.osvdb.org/40295>

SECUNIA: <http://secunia.com/advisories/28556>

SECUNIA: <http://secunia.com/advisories/28518>

CVE Reference: [CVE-2008-7234](#)

• **CVE-2008-7238 Oracle CVSS 2.0 Score = 6.0**

Multiple unspecified vulnerabilities in Oracle E-Business Suite 12.0.3 allow (1) local users to affect confidentiality and integrity via unknown vectors related to the Mobile Application Server component (APP01); (2) remote attackers to affect confidentiality via unknown vectors related to the Oracle Applications Framework (APP03); remote authenticated users to affect confidentiality and integrity via unknown vectors related to the (3) CRM Technical Foundation (APP05) and (4) Oracle Application Object Library (APP06); and remote authenticated users to affect integrity and availability via unknown vectors related to (5) Oracle Applications Technology Stack (APP07).

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

References:

CERT: <http://www.us-cert.gov/cas/techalerts/TA08-017A.html>
VUPEN: <http://www.vupen.com/english/advisories/2008/0180>
VUPEN: <http://www.vupen.com/english/advisories/2008/0150>
BID: <http://www.securityfocus.com/bid/27229>
CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuijan2008.html>
SECTRAK: <http://securitytracker.com/id?1019218>
HP: <http://marc.info/?l=bugtraq&m=120058413923005&w=2>
OSVDB: <http://www.osvdb.org/40290>
OSVDB: <http://www.osvdb.org/40289>
OSVDB: <http://www.osvdb.org/40288>
OSVDB: <http://www.osvdb.org/40286>
OSVDB: <http://www.osvdb.org/40284>
SECUNIA: <http://secunia.com/advisories/28556>
SECUNIA: <http://secunia.com/advisories/28518>
HP: <http://marc.info/?l=bugtraq&m=120058413923005&w=2>

CVE Reference: [CVE-2008-7238](#)

• **CVE-2008-7239 Oracle CVSS 2.0 Score = 5.0**

Multiple unspecified vulnerabilities in Oracle E-Business Suite 11.5.10.2 allow remote attackers to affect confidentiality via unknown vectors related to the (1) Oracle Application Object Library (APP02) and (2) Oracle Applications Manager (APP04).

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

References:

CERT: <http://www.us-cert.gov/cas/techalerts/TA08-017A.html>
VUPEN: <http://www.vupen.com/english/advisories/2008/0180>
VUPEN: <http://www.vupen.com/english/advisories/2008/0150>
BID: <http://www.securityfocus.com/bid/27229>
CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuijan2008.html>
SECTRAK: <http://securitytracker.com/id?1019218>
HP: <http://marc.info/?l=bugtraq&m=120058413923005&w=2>
HP: <http://marc.info/?l=bugtraq&m=120058413923005&w=2>
OSVDB: <http://www.osvdb.org/40287>
OSVDB: <http://www.osvdb.org/40285>
SECUNIA: <http://secunia.com/advisories/28556>
SECUNIA: <http://secunia.com/advisories/28518>

CVE Reference: [CVE-2008-7239](#)

• **CVE-2008-7235 Oracle CVSS 2.0 Score = 4.3**

Unspecified vulnerability in the Oracle Forms component in Oracle Application Server 10.1.2.2 and E-Business Suite 12.0.3 allows remote attackers to affect integrity via unknown vectors, aka AS04.

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

References:

CERT: <http://www.us-cert.gov/cas/techalerts/TA08-017A.html>

VUPEN: <http://www.vupen.com/english/advisories/2008/0180>

VUPEN: <http://www.vupen.com/english/advisories/2008/0150>

BID: <http://www.securityfocus.com/bid/27229>

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html>

HP: <http://marc.info/?l=bugtraq&m=120058413923005&w=2>

OSVDB: <http://www.osvdb.org/40296>

SECTRAK: <http://securitytracker.com/id?1019218>

SECUNIA: <http://secunia.com/advisories/28556>

SECUNIA: <http://secunia.com/advisories/28518>

HP: <http://marc.info/?l=bugtraq&m=120058413923005&w=2>

CVE Reference: [CVE-2008-7235](#)

• **CVE-2008-7236 Oracle CVSS 2.0 Score = 4.3**

Unspecified vulnerability in the Oracle JDeveloper component in Oracle Application Server 10.1.2.2 and 10.1.3.1 allows remote attackers to affect integrity via unknown vectors, aka AS05.

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

References:

CERT: <http://www.us-cert.gov/cas/techalerts/TA08-017A.html>

VUPEN: <http://www.vupen.com/english/advisories/2008/0180>

VUPEN: <http://www.vupen.com/english/advisories/2008/0150>

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html>

SECTRAK: <http://securitytracker.com/id?1019218>

HP: <http://marc.info/?l=bugtraq&m=120058413923005&w=2>

HP: <http://marc.info/?l=bugtraq&m=120058413923005&w=2>

BID: <http://www.securityfocus.com/bid/27229>

OSVDB: <http://www.osvdb.org/40297>

SECUNIA: <http://secunia.com/advisories/28556>

SECUNIA: <http://secunia.com/advisories/28518>

CVE Reference: [CVE-2008-7236](#)

• **CVE-2008-7237 Oracle CVSS 2.0 Score = 4.0**

Unspecified vulnerability in the Oracle Internet Directory component in Oracle Application Server 9.0.4.3 and 10.1.2.2 allows remote authenticated users to affect confidentiality via unknown vectors, aka AS06.

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

References:

CERT: <http://www.us-cert.gov/cas/techalerts/TA08-017A.html>

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html>

VUPEN: <http://www.vupen.com/english/advisories/2008/0180>

VUPEN: <http://www.vupen.com/english/advisories/2008/0150>

BID: <http://www.securityfocus.com/bid/27229>

OSVDB: <http://www.osvdb.org/40298>

SECTRAK: <http://securitytracker.com/id?1019218>

SECUNIA: <http://secunia.com/advisories/28556>

SECUNIA: <http://secunia.com/advisories/28518>

HP: <http://marc.info/?l=bugtraq&m=120058413923005&w=2>

HP: <http://marc.info/?l=bugtraq&m=120058413923005&w=2>

CVE Reference: [CVE-2008-7237](#)

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