

2009 Issue #3

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 v3.0.16 alpha](#) - Download Free WinRT v3.0.16 alpha installer by filling our download form. Size: 33MB

Download Here:

http://www.netvigilance.com/productdownloads?productname=winrt_setup_3_0_16

This Week in Review

New group points out the worst programming problems. Still security issues with taxpayer data. Phishing without emailing. A little story from real life.

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

• **DHS, Microsoft, others release Top 25 programming blunders**

A pair of prominent government agencies have teamed up with academic researchers and security software providers to get programmers more focused on security and buyers more clued in to what they're getting.

Experts from more than 30 U.S. and international cybersecurity organizations, including the Department of Homeland Security and National Security Agency, on Monday unveiled the Top 25 list of most dangerous programming errors, which often are leveraged to conduct cybercrime.

Two of the errors -- improper input validation and output encoding, which could be exploited to launch SQL injection attacks -- contributed to more than 1.5 million website breaches last year, according to the study's organizers, MITRE and the SANS Institute.

SC Magazine

Full Story :

<http://www.scmagazineus.com/DHS-Microsoft-others-release-Top-25-programming-blunders/article/123893/>

• Taxpayer data at IRS remains vulnerable, GAO warns

January 13, 2009 (Computerworld) Less than three months after the Treasury Inspector General for Tax Administration reported that there were major security vulnerabilities in two crucial Internal Revenue Service systems, the IRS's security practices have been panned by another government entity.

The report shows that taxpayer and other sensitive data continues to remain dangerously underprotected at the IRS. According to the GAO, while the IRS has addressed 49 of 115 previously reported security issues, several critical areas remain vulnerable.

A lot of the issues are the result of a continued failure by the IRS to implement any agency-wide information security program or review risk assessments annually, the GAO said. As a result, the agency remains "particularly vulnerable" to insider threats and malicious attacks that could expose financial and taxpayer data.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9125819&source=rss_topic1

• New phishing play exploits secure sessions to hijack data

Researchers have devised a new way for attackers to phish for credentials without the need to send emails or trick users into visiting a malicious website.

Dubbed "in-session" phishing by web security firm Trusteer, the conceptualized attack leverages a vulnerability present in all major browsers that allows attackers to learn if a user is logged into a banking site.

All criminals need to do is compromise a legitimate website with malicious JavaScript and wait for people to surf there, said Trusteer CTO Amit Klein. When users visit that site, the malcode will leverage a vulnerability in the way a certain function is implemented in popular browsers, he told SC MagazineUS.com on Monday.

SC Magazine

Full Story :

<http://www.scmagazineus.com/New-phishing-play-exploits-secure-sessions-to-hijack-data/article/123987/>

• Security Manager's Journal: Budget ax falls on disaster recovery

January 12, 2009 (Computerworld) I just came back from an all-day budgetary bloodbath. Not unexpectedly, my capital budget for 2009 for 2009 is basically zero.

In this day and age, I can't imagine any large company relying on a single point of failure for business-critical services. But that's exactly what our executives want to do. In their minds, duplicating our systems in a data center that may never get used essentially doubles the cost of any implementation.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=331934&source=rss_topic17

New Vulnerabilities Tested in SecureScout

• 16733 Oracle Enterprise Manager - Enterprise Config Management component unspecified Vulnerability (jul-2006/EM02)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html>

* MISC:

http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html

* HP: HPSBMA02133

<http://www.securityfocus.com/archive/1/archive/1/440758/100/100/threaded>

* CERT: TA06-200A

<http://www.us-cert.gov/cas/techalerts/TA06-200A.html>

* BID: 19054
<http://www.securityfocus.com/bid/19054>
* FRSIRT: ADV-2006-2863
<http://www.frsirt.com/english/advisories/2006/2863>
* FRSIRT: ADV-2006-2947
<http://www.frsirt.com/english/advisories/2006/2947>
* SECTRACK: 1016529
<http://securitytracker.com/id?1016529>
* SECUNIA: 21111
<http://secunia.com/advisories/21111>
* SECUNIA: 21165
<http://secunia.com/advisories/21165>
* XF: oracle-cpu-july-2006(27897)
<http://xforce.iss.net/xforce/xfdb/27897>

CVE Reference:

CVE-2006-3720 (cve.mitre.org, nvd.nist.gov)

• **16734 Oracle Enterprise Manager - Oracle Management Service component unspecified Vulnerability (jul-2006/EM03)**

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

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

References:

* CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html>
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
* HP: HPSBMA02133
<http://www.securityfocus.com/archive/1/archive/1/440758/100/100/threaded>
* CERT: TA06-200A
<http://www.us-cert.gov/cas/techalerts/TA06-200A.html>
* BID: 19054
<http://www.securityfocus.com/bid/19054>
* FRSIRT: ADV-2006-2863
<http://www.frsirt.com/english/advisories/2006/2863>
* FRSIRT: ADV-2006-2947
<http://www.frsirt.com/english/advisories/2006/2947>
* SECTRACK: 1016529
<http://securitytracker.com/id?1016529>
* SECUNIA: 21111
<http://secunia.com/advisories/21111>
* SECUNIA: 21165
<http://secunia.com/advisories/21165>
* XF: oracle-cpu-july-2006(27897)
<http://xforce.iss.net/xforce/xfdb/27897>

CVE Reference:

CVE-2006-3721 (cve.mitre.org, nvd.nist.gov)

• **16735 Oracle Enterprise Manager - Oracle Management Service component unspecified Vulnerability (jul-2006/EM04)**

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

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

References:

* CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html>
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
* HP: HPSBMA02133
<http://www.securityfocus.com/archive/1/archive/1/440758/100/100/threaded>
* CERT: TA06-200A

<http://www.us-cert.gov/cas/techalerts/TA06-200A.html>

* BID: 19054

<http://www.securityfocus.com/bid/19054>

* FRSIRT: ADV-2006-2863

<http://www.frsirt.com/english/advisories/2006/2863>

* FRSIRT: ADV-2006-2947

<http://www.frsirt.com/english/advisories/2006/2947>

* SECTRACK: 1016529

<http://securitytracker.com/id?1016529>

* SECUNIA: 21111

<http://secunia.com/advisories/21111>

* SECUNIA: 21165

<http://secunia.com/advisories/21165>

* XF: oracle-cpu-july-2006(27897)

<http://xforce.iss.net/xforce/xfdb/27897>

CVE Reference:

CVE-2006-3721 (cve.mitre.org, nvd.nist.gov)

• 16737 Oracle Enterprise Manager - CORE: Reporting Framework component unspecified Vulnerability (apr-2006/EM01)

An unspecified vulnerability with unknown impact exists in Oracle Enterprise Manager CORE: Reporting Framework component.

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

References:

* CONFIRM:

<http://www.oracle.com/technology/Deploy/security/pdf/cpuapr2006.html>

* HP: HPSBMA02113

<http://www.securityfocus.com/archive/1/archive/1/432267/100/0/threaded>

* CERT-VN: VU#443265

<http://www.kb.cert.org/vuls/id/443265>

* BID: 17590

<http://www.securityfocus.com/bid/17590>

* FRSIRT: ADV-2006-1397

<http://www.frsirt.com/english/advisories/2006/1397>

* FRSIRT: ADV-2006-1571

<http://www.frsirt.com/english/advisories/2006/1571>

* SECTRACK: 1015961

<http://securitytracker.com/id?1015961>

* SECUNIA: 19712

<http://secunia.com/advisories/19712>

* SECUNIA: 19859

<http://secunia.com/advisories/19859>

* XF: oracle-reporting-framework-access(26056)

<http://xforce.iss.net/xforce/xfdb/26056>

CVE Reference:

CVE-2006-1885 (cve.mitre.org, nvd.nist.gov)

• 16738 Oracle Enterprise Manager - CORE: Reporting Framework component unspecified Vulnerability (apr-2006/EM02)

An unspecified vulnerability with unknown impact exists in Oracle Enterprise Manager CORE: Reporting Framework component.

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

References:

* CONFIRM:

<http://www.oracle.com/technology/Deploy/security/pdf/cpuapr2006.html>

* HP: HPSBMA02113

<http://www.securityfocus.com/archive/1/archive/1/432267/100/0/threaded>

* CERT-VN: VU#443265

<http://www.kb.cert.org/vuls/id/443265>

* BID: 17590

<http://www.securityfocus.com/bid/17590>

- * FRSIRT: ADV-2006-1397
<http://www.frsirt.com/english/advisories/2006/1397>
- * FRSIRT: ADV-2006-1571
<http://www.frsirt.com/english/advisories/2006/1571>
- * SECTRACK: 1015961
<http://securitytracker.com/id?1015961>
- * SECUNIA: 19712
<http://secunia.com/advisories/19712>
- * SECUNIA: 19859
<http://secunia.com/advisories/19859>
- * XF: oracle-reporting-framework-access(26056)
<http://xforce.iss.net/xforce/xfdb/26056>

CVE Reference:

CVE-2006-1885 (cve.mitre.org, nvd.nist.gov)

● **16775 Oracle Enterprise Manager - Oracle Agent component unspecified Vulnerability (oct-2005/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/pdf/cpuoct2005.html>
- * CERT: TA05-292A
<http://www.us-cert.gov/cas/techalerts/TA05-292A.html>
- * CERT-VN: VU#210524
<http://www.kb.cert.org/vuls/id/210524>
- * CERT-VN: VU#865948
<http://www.kb.cert.org/vuls/id/865948>
- * BID: 15134
<http://www.securityfocus.com/bid/15134>
- * SECUNIA: 17250
<http://secunia.com/advisories/17250>

CVE Reference:

CVE-2005-3460 (cve.mitre.org, nvd.nist.gov)

● **18252 HTTP TRACK method, Cross-Site Tracing Vulnerability**

TRACK is an HTTP method available in version 1.1 of the HTTP protocol. This method is usually available by default on HTTP servers. The purpose of this method is to echo client requests.

This method can be used to retrieve information sent by the client in the HTTP headers. As browsers do not support methods other than GET and POST, special techniques are required to exploit the vulnerability like the use of ActiveX.

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

References:

- * CERT-VN: Microsoft Internet Information Server (IIS) vulnerable to cross-site scripting via HTTP TRACK method
<http://www.kb.cert.org/vuls/id/288308>
- * MISC: Microsoft IIS Logging Failure
<http://www.aqtronix.com/Advisories/AQ-2003-02.txt>
- * MISC: HTTP Track Request
http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=20419
- * BID: 9313
<http://www.securityfocus.com/bid/9313/>
- * OSVDB: Multiple Web Server Dangerous HTTP Method TRACK
<http://osvdb.org/show/osvdb/5648>

CVE Reference:

● **18253 SMB Buffer Overflow Remote Code Execution Vulnerability (MS09-001/958687) (Remote File Checking)**

An unauthenticated remote code execution vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a

computer running the Server service. An attacker who successfully exploited this vulnerability could take complete control of the system. Most attempts to exploit this vulnerability would result in a system denial of service condition, however remote code execution is theoretically possible.

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

References:

- * SECUNIA: 31883
<http://secunia.com/advisories/31883/>
- * BID: 33121
<http://www.securityfocus.com/bid/33121>
- * SECTRACK: 1021560
<http://securitytracker.com/alerts/2009/Jan/1021560.html>
- * MS: ms09-001
<http://www.microsoft.com/technet/security/bulletin/ms09-001.msp>

CVE Reference:

CVE-2008-4834 (cve.mitre.org, nvd.nist.gov)

• 18254 SMB Validation Remote Code Execution Vulnerability (MS09-001/958687) (Remote File Checking)

An unauthenticated remote code execution vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the Server service. An attacker who successfully exploited this vulnerability could cause the attacker to take complete control of the system. Most attempts to exploit this vulnerability would result in a system denial of service condition, however remote code execution is theoretically possible.

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

References:

- * SECUNIA: 31883
<http://secunia.com/advisories/31883/>
- * BID: 33122
<http://www.securityfocus.com/bid/33122>
- * SECTRACK: 1021560
<http://securitytracker.com/alerts/2009/Jan/1021560.html>
- * MS: ms09-001
<http://www.microsoft.com/technet/security/bulletin/ms09-001.msp>

CVE Reference:

CVE-2008-4835 (cve.mitre.org, nvd.nist.gov)

• 18255 SMB Validation Denial of Service Vulnerability (MS09-001/958687) (Remote File Checking)

A denial of service vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the Server service. An attacker who successfully exploited this vulnerability could cause the computer to stop responding and restart.

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

References:

- * SECUNIA: 31883
<http://secunia.com/advisories/31883/>
- * BID: 31179
<http://www.securityfocus.com/bid/31179>
- * SECTRACK: 1021560
<http://securitytracker.com/alerts/2009/Jan/1021560.html>
- * MS: ms09-001
<http://www.microsoft.com/technet/security/bulletin/ms09-001.msp>

CVE Reference:

CVE-2008-4114 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-4834 Microsoft CVSS 2.0 Score = 10.0

Buffer overflow in SMB in the Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via malformed values of unspecified "fields inside the SMB packets" in an NT Trans request, aka "SMB Buffer Overflow Remote Code Execution Vulnerability."

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

References:

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-001.msp>

CVE Reference: [CVE-2008-4834](#)

• CVE-2008-4835 Microsoft CVSS 2.0 Score = 10.0

SMB in the Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to execute arbitrary code via malformed values of unspecified "fields inside the SMB packets" in an NT Trans2 request, related to "insufficiently validating the buffer size," aka "SMB Validation Remote Code Execution Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-001.msp>

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>

CVE Reference: [CVE-2008-4835](#)

• CVE-2009-0119 Microsoft CVSS 2.0 Score = 10.0

Buffer overflow in Microsoft Windows XP SP3 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a crafted .chm file.

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

References:

BID: <http://www.securityfocus.com/bid/33204>

MILWORM: <http://www.milw0rm.com/exploits/7720>

CVE Reference: [CVE-2009-0119](#)

• CVE-2008-4006 Oracle CVSS 2.0 Score = 10.0

Unspecified vulnerability in the Oracle Secure Backup component in Oracle Secure Backup 10.1.0.3 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

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

References:

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

CVE Reference: [CVE-2008-4006](#)

• CVE-2008-5444 Oracle CVSS 2.0 Score = 10.0

Unspecified vulnerability in the Oracle Secure Backup component in Oracle Secure Backup 10.2.0.2 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

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

References:

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

CVE Reference: [CVE-2008-5444](#)

• **CVE-2008-5448 Oracle CVSS 2.0 Score = 10.0**

Unspecified vulnerability in the Oracle Secure Backup component in Oracle Secure Backup 10.2.0.2 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

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

References:

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

CVE Reference: [CVE-2008-5448](#)

• **CVE-2008-5449 Oracle CVSS 2.0 Score = 10.0**

Unspecified vulnerability in the Oracle Secure Backup component in Oracle Secure Backup 10.2.0.2 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

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

References:

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

CVE Reference: [CVE-2008-5449](#)

• **CVE-2008-5457 Oracle CVSS 2.0 Score = 10.0**

Unspecified vulnerability in the Oracle BEA WebLogic Server Plugins for Apache, Sun and IIS web servers component in BEA Product Suite 10.3, 10.0, MP1, 9.2, MP3, 9.1, 9.0, 8.1, SP6, 7.0, and SP7 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

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

References:

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

CVE Reference: [CVE-2008-5457](#)

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