

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

SecureScout receives good review. Cloud computing vendors need to be audited. Social networks spread malware. Recession cutting into IT budgets.

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

• netVigilance SecureScout NX

The netVigilance SecureScout NX is a network vulnerability scanning tool that at first glance looks like a scanning tool from times past. However, this product packs a serious punch. The SecureScout can scan almost anything that has an IP address - be it firewalls, routers, operating systems or anything else you can find to throw at it. The tool can also do in-depth firewall testing and scan multiple subnets from one console. All this functionality should be hard to use, right? Not at all. This product installed in minutes and we were scanning not long after that. The application interface is quite simple and very intuitive to navigate. There is a list of various scans, tests and exploits along the left-hand side grouped into categories in a tree structure. Scan results are displayed in a separate pane showing information about various target machines. If these machines are clicked on, more detailed information is shown. SC Magazine

Full Story :

<http://www.scmagazineus.com/netVigilance-SecureScout-NX/Review/2840/>

• Cloud computing providers require strong audits

Companies must develop better ways of evaluating the security and privacy practices of the cloud services they utilize, according to a report by Forrester released Friday.

"Auditing the cloud providers is something that needs to be done since you're essentially giving your data into the good hands of the providers," Philippe Courtot, chairman and CEO, Qualys told SCmagazineUS.com Monday.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Cloud-computing-providers-require-strong-audits/article/136580/>

• **Malware most potent on social networks**

Malware distributed via social networking sites is 10 times more effective than malware spread via email, according to Kaspersky Lab Global Research.

This has enormous implications for the future of social networking, because the popularity of social networking sites has not been ignored by cybercriminals. Last year, sites such as Facebook and Twitter became hotbeds of malware and spam -- and yet another source of illegal gains on the internet, Tanase said.

It doesn't help that social networking users trust other users and accept messages from people on their friends list almost without thinking, Tanase said. This makes it easy for cybercriminals to spread links to infected sites.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Malware-most-potent-on-social-networks/article/136659/>

• **Nearly half of IT security budgets deemed insufficient**

It's no news that the current economic situation has put a strain on companies' finances, but a recent survey aimed to quantify the toll the recession has taken on IT budgets.

A sixth annual survey, called "What keeps network administrators up at night" conducted in late April was commissioned by VanDyke Software and executed by survey research organization Amplitude Research. The survey of 320 network and system administrators nationwide found that 41 percent said their company's overall IT budget has decreased - compared to 18 percent last year. Some 21.2 percent saw their IT security budget decrease by more than 10 percent and 12.18 percent said their decrease was less than 10 percent, Steve Birnkrant, CEO of Amplitude Research told SCMagazineUS.com Wednesday.

In addition, nearly half (46 percent) of respondents said they believe their organization has not sufficiently budgeted to support their current information security needs.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Nearly-half-of-IT-security-budgets-deemed-insufficient/article/136727/>

New Vulnerabilities Tested in SecureScout

• **18364 Blended Threat Elevation of Privilege Vulnerability (MS09-015/959426) (Remote File Checking)**

A blended threat elevation of privilege vulnerability exists in the way the SearchPath function in Windows locates and opens files on the system. An attacker could exploit the vulnerability by convincing a user to download a specially crafted file to a specific location, and then open an application that could load the file under certain circumstances.

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

References:

* MISC:

<http://aviv.affon.net/2008/05/31/SafariPwnsInternetExplorer.aspx>

* MISC:

<http://blogs.zdnet.com/security/?p=1230>

* MISC:

http://www.dhanjani.com/archives/2008/05/safari_carpet_bomb.html

* MISC:

<http://www.microsoft.com/technet/security/advisory/953818.msp>

* CONFIRM:

<http://support.avaya.com/elmodocs2/security/ASA-2009-133.htm>

* APPLE: APPLE-SA-2008-06-19

<http://lists.apple.com/archives/security-announce/2008/Jun/msg00001.html>

* MS: MS09-015

<http://www.microsoft.com/technet/security/bulletin/ms09-015.msp>

* CERT: TA09-104A

<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>

* BID: 29445

<http://www.securityfocus.com/bid/29445>

* SECTrack: 1022047

<http://www.securitytracker.com/id?1022047>

* VUPEN: ADV-2008-1706

<http://www.frsirt.com/english/advisories/2008/1706>

* SECTrack: 1020150

<http://securitytracker.com/id?1020150>

* SECUNIA: 30467

<http://secunia.com/advisories/30467>

* VUPEN: ADV-2009-1028

<http://www.vupen.com/english/advisories/2009/1028>

* VUPEN: ADV-2009-1029

<http://www.vupen.com/english/advisories/2009/1029>

* XF: apple-safari-windows-code-execution(42765)

<http://xforce.iss.net/xforce/xfdb/42765>

CVE Reference:

CVE-2008-2540 (cve.mitre.org, nvd.nist.gov)

• 18369 Oracle Application Server - Outside In Technology component unspecified Vulnerability (apr-2009/CVE-2009-1009)

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Outside In Technology" component.

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>

* CERT: TA09-105A

<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>

* OSVDB: 53748

<http://osvdb.org/53748>

* SECTrack: 1022055

<http://www.securitytracker.com/id?1022055>

* SECUNIA: 34693

<http://secunia.com/advisories/34693>

CVE Reference:

CVE-2009-1009 (cve.mitre.org, nvd.nist.gov)

• 18370 Oracle Application Server - Outside In Technology component unspecified Vulnerability (apr-2009/CVE-2009-1010)

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Outside In Technology" component.

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>

* CERT: TA09-105A

<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>

* OSVDB: 53749

<http://osvdb.org/53749>

* SECTrack: 1022055

<http://www.securitytracker.com/id?1022055>

* SECUNIA: 34693

<http://secunia.com/advisories/34693>

CVE Reference:

CVE-2009-1010 (cve.mitre.org, nvd.nist.gov)

• 18371 Oracle Application Server - Outside In Technology component unspecified Vulnerability (apr-2009/CVE-2009-1011)

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Outside In Technology" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>
- * CERT: TA09-105A
<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>
- * OSVDB: 53750
<http://osvdb.org/53750>
- * SECTRACK: 1022055
<http://www.securitytracker.com/id?1022055>
- * SECUNIA: 34693
<http://secunia.com/advisories/34693>

CVE Reference:

CVE-2009-1011 (cve.mitre.org, nvd.nist.gov)

• 18372 Oracle Application Server - Portal component unspecified Vulnerability (apr-2009/CVE-2009-0974)

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

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>
- * CERT: TA09-105A
<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>
- * OSVDB: 53751
<http://osvdb.org/53751>
- * SECTRACK: 1022055
<http://www.securitytracker.com/id?1022055>
- * SECUNIA: 34693
<http://secunia.com/advisories/34693>

CVE Reference:

CVE-2009-0974 (cve.mitre.org, nvd.nist.gov)

• 18373 Oracle Application Server - Portal component unspecified Vulnerability (apr-2009/CVE-2009-0983)

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

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>
- * CERT: TA09-105A
<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>
- * OSVDB: 53752
<http://osvdb.org/53752>
- * SECTRACK: 1022055
<http://www.securitytracker.com/id?1022055>
- * SECUNIA: 34693
<http://secunia.com/advisories/34693>

CVE Reference:

CVE-2009-0983 (cve.mitre.org, nvd.nist.gov)

• **18374 Oracle Application Server - BI Publisher component unspecified Vulnerability (apr-2009/CVE-2009-0994)**

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

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>
- * CERT: TA09-105A
<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>
- * OSVDB: 53744
<http://osvdb.org/53744>
- * SECTrack: 1022055
<http://www.securitytracker.com/id?1022055>
- * SECUNIA: 34693
<http://secunia.com/advisories/34693>

CVE Reference:

CVE-2009-0994 (cve.mitre.org, nvd.nist.gov)

• **18375 Oracle Application Server - BI Publisher component unspecified Vulnerability (apr-2009/CVE-2009-0996)**

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

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>
- * CERT: TA09-105A
<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>
- * OSVDB: 53745
<http://osvdb.org/53745>
- * SECTrack: 1022055
<http://www.securitytracker.com/id?1022055>
- * SECUNIA: 34693
<http://secunia.com/advisories/34693>

CVE Reference:

CVE-2009-0996 (cve.mitre.org, nvd.nist.gov)

• **18376 Oracle Application Server - BI Publisher component unspecified Vulnerability (apr-2009/CVE-2009-1017)**

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

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>
- * CERT: TA09-105A
<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>
- * OSVDB: 53746
<http://osvdb.org/53746>
- * SECTrack: 1022055
<http://www.securitytracker.com/id?1022055>
- * SECUNIA: 34693
<http://secunia.com/advisories/34693>

CVE Reference:

CVE-2009-1017 (cve.mitre.org, nvd.nist.gov)

• **18377 Microsoft Office PowerPoint Legacy File Format Vulnerability (CVE-2009-0220) (MS09-017/967340) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

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

References:

* MS: MS09-017
<http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>

CVE Reference:

CVE-2009-0220 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2009-1131 Microsoft CVSS 2.0 Score = 10.0**

Multiple stack-based buffer overflows in Microsoft Office PowerPoint 2000 SP3 allow remote attackers to execute arbitrary code via a large amount of data associated with unspecified atoms in a PowerPoint file that triggers memory corruption, aka "Data Out of Bounds Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>

MISC: http://secunia.com/secunia_research/2008-46/

CVE Reference: [CVE-2009-1131](http://cve.mitre.org/cve/2009/1131)

• **CVE-2009-1137 Microsoft CVSS 2.0 Score = 9.4**

Microsoft Office PowerPoint 2000 SP3, 2002 SP3, and 2003 SP3 allows remote attackers to execute arbitrary code via crafted sound data in a file that uses a PowerPoint 4.0 native file format, leading to memory corruption, aka "Legacy File Format Vulnerability," a different vulnerability than CVE-2009-0222, CVE-2009-0223, CVE-2009-0226, and CVE-2009-0227.

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>

CVE Reference: [CVE-2009-1137](http://cve.mitre.org/cve/2009/1137)

• **CVE-2009-0220 Microsoft CVSS 2.0 Score = 9.3**

Multiple stack-based buffer overflows in the PowerPoint 4.0 importer (PP4X32.DLL) in Microsoft Office PowerPoint 2000 SP3, 2002 SP3, and 2003 SP3 allow remote attackers to execute arbitrary code via crafted formatting data for paragraphs in a file that uses a PowerPoint 4.0 native file format, related to (1) an incorrect calculation from a record header, or (2) an interget that is used to specify the number of bytes to copy, aka "Legacy File Format Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>

CVE Reference: [CVE-2009-0220](http://cve.mitre.org/cve/2009/0220)

• **CVE-2009-0221 Microsoft CVSS 2.0 Score = 9.3**

Integer overflow in Microsoft Office PowerPoint 2002 SP3 and 2003 SP3 allows remote attackers to execute arbitrary code via an invalid record type in a PowerPoint file that triggers memory corruption, aka "Integer Overflow Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>

CVE Reference: [CVE-2009-0221](#)

• **CVE-2009-0222 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office PowerPoint 2000 SP3, 2002 SP3, and 2003 SP3 allows remote attackers to execute arbitrary code via crafted sound data in a file that uses a PowerPoint 4.0 native file format, leading to a "pointer overwrite" and memory corruption, aka "Legacy File Format Vulnerability," a different vulnerability than CVE-2009-0223, CVE-2009-0226, CVE-2009-0227, and CVE-2009-1137.

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>

MISC:

http://www.vupen.com/exploits/Microsoft_PowerPoint_Pointer_Overwrite_Code_Execution_Exploit_MS09_017_1290123.php

MISC:

http://www.vupen.com/exploits/Microsoft_PowerPoint_Memory_Corruption_Code_Execution_Exploit_MS09_017_1290124.php

CVE Reference: [CVE-2009-0222](#)

• **CVE-2009-0223 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office PowerPoint 2000 SP3, 2002 SP3, and 2003 SP3 allows remote attackers to execute arbitrary code via crafted sound data in a file that uses a PowerPoint 4.0 native file format, leading to memory corruption, aka "Legacy File Format Vulnerability," a different vulnerability than CVE-2009-0222, CVE-2009-0226, CVE-2009-0227, and CVE-2009-1137.

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>

CVE Reference: [CVE-2009-0223](#)

• **CVE-2009-0224 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office PowerPoint 2000 SP3, 2002 SP3, 2003 SP3, and 2007 SP1 and SP2; PowerPoint Viewer 2003 and 2007 SP1 and SP2; PowerPoint in Microsoft Office 2004 for Mac and 2008 for Mac; Open XML File Format Converter for Mac; Microsoft Works 8.5 and 9.0; and Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2 do not properly validate list records in PowerPoint files, which allows remote attackers to execute arbitrary code via a crafted file that triggers memory corruption related to an invalid record type, aka "Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>

CVE Reference: [CVE-2009-0224](#)

• **CVE-2009-0225 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office PowerPoint 2002 SP3 allows remote attackers to execute arbitrary code via crafted sound data in a file that uses a PowerPoint 95 native file format, leading to improper "array indexing" and memory corruption, aka "PP7 Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>

MISC:

http://www.vupen.com/exploits/Microsoft_PowerPoint_Array_Indexing_Code_Execution_Exploit_MS09_017_1290125.php

CVE Reference: [CVE-2009-0225](#)

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