

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 study looks at website risks. New group to advice PCI Security Council. New group formed to fight malware.

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

• Website risks highlighted in two new studies

Two reports released this week confirmed the tidal shift in the type of websites into which cybercriminals are injecting malware.

WhiteHat Security, in the seventh installment of its Website Security Statistics Report, to be released on Tuesday, found that 82 percent of websites studied over the past year have had a "high," "critical," or "urgent" issueduring their lifetime, with cross-site scripting continuing to top the list.

WhiteHat's report is no more alarming than in the past two years, Jeremiah Grossman, founder and CTO of the company, told SCMagazineUS.com on Monday. But this time, most of the more than 1,000 compromised websites reviewed in the report belong to well-known brands.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Website-risks-highlighted-in-two-new-studies/article/137005/>

• PCI appoints new board of advisers

A roster of new organizations will make up the second Payment Card Industry Security Standards Council (PCI SSC) board of advisers, including Bank of America, Wal-Mart and PayPal, the industry standards body announced Monday.

The advisers will replace the inaugural board, which served a two-year term beginning in 2007. The purpose of the board is to provide strategic and technical guidance to the PCI SSC, which manages the Payment Card Industry Data Security Standard (PCI DSS).

The new board's first task will be reviewing the results of an emerging technology study that was commissioned by the council, according to a PCI news release.

SC Magazine

Full Story :

<http://www.scmagazineus.com/PCI-appoints-new-board-of-advisers/article/137025/>

• "Chain of Trust" initiative launched to fight malware

A group of cybersecurity advocacy organizations have teamed up to fight malware on the web.

The Anti-Spyware Coalition (ASC), National Cyber Security Alliance (NCSA), and StopBadware.org announced their collaboration, known as the Chain of Trust Initiative, Tuesday at the ASC workshop in Washington.

The goal of the partnership is to map the threats by identifying attack vectors and appropriate solutions, Ari Schwartz, ASC coordinator and vice president of the Center for Democracy and Technology (CDT), a nonprofit public interest group, told SCMagazineUS.com Tuesday. The effort has involved security companies, independent researchers, webmasters, registrars, hosting companies, network providers, and enforcement agencies, the organizations said in a news release.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Chain-of-Trust-initiative-launched-to-fight-malware/article/137079/>

New Vulnerabilities Tested in SecureScout

• 18378 Microsoft Office PowerPoint Integer Overflow Vulnerability (CVE-2009-0221) (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>

* CERT: TA09-132A

<http://www.us-cert.gov/cas/techalerts/TA09-132A.html>

* BID: 34835

<http://www.securityfocus.com/bid/34835>

* OSVDB: 54394

<http://osvdb.org/54394>

* SECTRACK: 1022205

<http://www.securitytracker.com/id?1022205>

* SECUNIA: 32428

<http://secunia.com/advisories/32428>

* VUPEN: ADV-2009-1290

<http://www.vupen.com/english/advisories/2009/1290>

CVE Reference:

CVE-2009-0221 (cve.mitre.org, nvd.nist.gov)

• 18379 Microsoft Office PowerPoint Legacy File Format Vulnerability (CVE-2009-0222) (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:

* MISC:

[http://www.vupen.com/exploits/Microsoft PowerPoint Memory Corruption Code Execution Exploit MS09 017 1290124](http://www.vupen.com/exploits/Microsoft_PowerPoint_Memory_Corruption_Code_Execution_Exploit_MS09_017_1290124)

* MISC:

[http://www.vupen.com/exploits/Microsoft PowerPoint Pointer Overwrite Code Execution Exploit MS09 017 1290123](http://www.vupen.com/exploits/Microsoft_PowerPoint_Pointer_Overwrite_Code_Execution_Exploit_MS09_017_1290123)

* MS: MS09-017

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

* CERT: TA09-132A

<http://www.us-cert.gov/cas/techalerts/TA09-132A.html>

* BID: 34831

<http://www.securityfocus.com/bid/34831>

* OSVDB: 54382

<http://osvdb.org/54382>

* SECTRACK: 1022205

<http://www.securitytracker.com/id?1022205>

* SECUNIA: 32428

<http://secunia.com/advisories/32428>

* VUPEN: ADV-2009-1290

<http://www.vupen.com/english/advisories/2009/1290>

CVE Reference:

CVE-2009-0222 (cve.mitre.org, nvd.nist.gov)

● 18380 Microsoft Office PowerPoint Legacy File Format Vulnerability (CVE-2009-0223) (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>

* CERT: TA09-132A

<http://www.us-cert.gov/cas/techalerts/TA09-132A.html>

* BID: 34834

<http://www.securityfocus.com/bid/34834>

* SECTRACK: 1022205

<http://www.securitytracker.com/id?1022205>

* SECUNIA: 32428

<http://secunia.com/advisories/32428>

* VUPEN: ADV-2009-1290

<http://www.vupen.com/english/advisories/2009/1290>

CVE Reference:

CVE-2009-0223 (cve.mitre.org, nvd.nist.gov)

● 18381 Microsoft Office PowerPoint Memory Corruption Vulnerability (CVE-2009-0224) (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>

* CERT: TA09-132A

<http://www.us-cert.gov/cas/techalerts/TA09-132A.html>

* BID: 34879
<http://www.securityfocus.com/bid/34879>
* SECTRACK: 1022205
<http://www.securitytracker.com/id?1022205>
* SECUNIA: 32428
<http://secunia.com/advisories/32428>
* VUPEN: ADV-2009-1290
<http://www.vupen.com/english/advisories/2009/1290>

CVE Reference:

CVE-2009-0224 (cve.mitre.org, nvd.nist.gov)

• **18382 Microsoft Office PowerPoint PP7 Memory Corruption Vulnerability (CVE-2009-0225) (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:

* MISC:
http://www.vupen.com/exploits/Microsoft_PowerPoint_Array_Indexing_Code_Execution_Exploit_MS09_017_1290125.php
* MS: MS09-017
<http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>
* CERT: TA09-132A
<http://www.us-cert.gov/cas/techalerts/TA09-132A.html>
* BID: 34880
<http://www.securityfocus.com/bid/34880>
* OSVDB: 54388
<http://osvdb.org/54388>
* SECTRACK: 1022205
<http://www.securitytracker.com/id?1022205>
* SECUNIA: 32428
<http://secunia.com/advisories/32428>
* VUPEN: ADV-2009-1290
<http://www.vupen.com/english/advisories/2009/1290>

CVE Reference:

CVE-2009-0225 (cve.mitre.org, nvd.nist.gov)

• **18383 Microsoft Office PowerPoint Legacy File Format Vulnerability (CVE-2009-0226) (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:

* IDEFENSE: 20090512 Microsoft PowerPoint 4.2 Conversion Filter Stack Overflow
<http://labs.odefense.com/intelligence/vulnerabilities/display.php?id=789>
* MS: MS09-017
<http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>
* CERT: TA09-132A
<http://www.us-cert.gov/cas/techalerts/TA09-132A.html>
* BID: 34881
<http://www.securityfocus.com/bid/34881>
* SECTRACK: 1022205
<http://www.securitytracker.com/id?1022205>
* SECUNIA: 32428
<http://secunia.com/advisories/32428>
* VUPEN: ADV-2009-1290
<http://www.vupen.com/english/advisories/2009/1290>

CVE Reference:

CVE-2009-0226 (cve.mitre.org, nvd.nist.gov)

● **18384 Microsoft Office PowerPoint Legacy File Format Vulnerability (CVE-2009-0227) (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:

- * IDEFENSE: 20090512 Microsoft PowerPoint 4.2 Conversion Filter Stack Buffer Overflow Vulnerability
<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=787>
- * MS: MS09-017
<http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>
- * CERT: TA09-132A
<http://www.us-cert.gov/cas/techalerts/TA09-132A.html>
- * BID: 34882
<http://www.securityfocus.com/bid/34882>
- * OSVDB: 54384
<http://osvdb.org/54384>
- * SECTRACK: 1022205
<http://www.securitytracker.com/id?1022205>
- * SECUNIA: 32428
<http://secunia.com/advisories/32428>
- * VUPEN: ADV-2009-1290
<http://www.vupen.com/english/advisories/2009/1290>

CVE Reference:

CVE-2009-0227 (cve.mitre.org, nvd.nist.gov)

● **18385 Microsoft Office PowerPoint Memory Corruption Vulnerability (CVE-2009-0556) (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:

- * CONFIRM:
<http://blogs.technet.com/mmpc/archive/2009/04/02/new-0-day-exploits-using-powerpoint-files.aspx>
- * CONFIRM:
<http://blogs.technet.com/msrc/archive/2009/04/02/microsoft-security-advisory-969136.aspx>
- * CONFIRM:
<http://blogs.technet.com/srd/archive/2009/04/02/investigating-the-new-powerpoint-issue.aspx>
- * CONFIRM:
<http://www.microsoft.com/technet/security/advisory/969136.msp>
- * MS: MS09-017
<http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>
- * CERT: TA09-132A
<http://www.us-cert.gov/cas/techalerts/TA09-132A.html>
- * CERT-VN: VU#627331
<http://www.kb.cert.org/vuls/id/627331>
- * BID: 34351
<http://www.securityfocus.com/bid/34351>
- * OSVDB: 53182
<http://osvdb.org/53182>
- * SECTRACK: 1021967
<http://www.securitytracker.com/id?1021967>
- * SECUNIA: 34572
<http://secunia.com/advisories/34572>
- * VUPEN: ADV-2009-0915
<http://www.vupen.com/english/advisories/2009/0915>
- * VUPEN: ADV-2009-1290
<http://www.vupen.com/english/advisories/2009/1290>
- * XF: powerpoint-undefined-code-execution(49632)
<http://xforce.iss.net/xforce/xfdb/49632>

CVE Reference:

CVE-2009-0556 (cve.mitre.org, nvd.nist.gov)

• **18386 Microsoft Office PowerPoint PP7 Memory Corruption Vulnerability (CVE-2009-1128) (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>
- * CERT: TA09-132A
<http://www.us-cert.gov/cas/techalerts/TA09-132A.html>
- * BID: 34837
<http://www.securityfocus.com/bid/34837>
- * SECTRACK: 1022205
<http://www.securitytracker.com/id?1022205>
- * SECUNIA: 32428
<http://secunia.com/advisories/32428>
- * VUPEN: ADV-2009-1290
<http://www.vupen.com/english/advisories/2009/1290>

CVE Reference:

CVE-2009-1128 (cve.mitre.org, nvd.nist.gov)

• **18387 Microsoft Office PowerPoint PP7 Memory Corruption Vulnerability (CVE-2009-1129) (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:

- * IDEFENSE: 20090512 Microsoft PowerPoint PPT95 Import Multiple Stack Buffer Overflow Vulnerabilities
<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=791>
- * MS: MS09-017
<http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>
- * CERT: TA09-132A
<http://www.us-cert.gov/cas/techalerts/TA09-132A.html>
- * BID: 34839
<http://www.securityfocus.com/bid/34839>
- * OSVDB: 54387
<http://osvdb.org/54387>
- * SECTRACK: 1022205
<http://www.securitytracker.com/id?1022205>
- * SECUNIA: 32428
<http://secunia.com/advisories/32428>
- * VUPEN: ADV-2009-1290
<http://www.vupen.com/english/advisories/2009/1290>

CVE Reference:

CVE-2009-1129 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2009-1676 Microsoft CVSS 2.0 Score = 7.6**

The WebDAV implementation in Microsoft Internet Information Services (IIS) 6.0 allows remote attackers to bypass URI-based protection mechanisms, and list folders or read, create, or modify files, via a %c0%af (Unicode / character) at an arbitrary position in the URI, as demonstrated by inserting %c0%af into a "/protected/" initial pathname component to bypass the password protection on the protected\ folder.

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

References:

MISC: <http://view.samurajdata.se/psview.php?id=023287d6&page=1>

MISC: <http://isc.sans.org/diary.html?n&storyid=6397>

MISC: <http://blog.zoller.lu/2009/05/iis-6-webdac-auth-bypass-and-data.html>

MISC: http://archives.neohapsis.com/archives/fulldisclosure/2009-05/att-0135/IIS_Advisory.pdf

FULLDISC: <http://archives.neohapsis.com/archives/fulldisclosure/2009-05/0144.html>

FULLDISC: <http://archives.neohapsis.com/archives/fulldisclosure/2009-05/0139.html>

FULLDISC: <http://archives.neohapsis.com/archives/fulldisclosure/2009-05/0135.html>

CVE Reference: [CVE-2009-1676](#)

• CVE-2009-0721 HP CVSS 2.0 Score = 10.0

Unspecified vulnerability in Easy Login in the Sender module in HP Remote Graphics Software (RGS) 4.0.0 through 5.2.4 allows remote attackers to execute arbitrary code via unknown vectors.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/1323>

SECTRAK: <http://securitytracker.com/id?1022221>

BID: <http://www.securityfocus.com/bid/34980>

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01731970

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01731970

SECUNIA: <http://secunia.com/advisories/35089>

SECUNIA: <http://secunia.com/advisories/35087>

CVE Reference: [CVE-2009-0721](#)

• CVE-2009-1418 HP CVSS 2.0 Score = 4.3

Cross-site scripting (XSS) vulnerability in HP System Management Homepage (SMH) before 3.0.1.73 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. Per: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01745065> "SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP System Management Homepage (SMH) before v3.0.1.73 running on Linux and Windows Server 2003, 2008."

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

References:

SECTRAK: <http://securitytracker.com/id?1022242>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01745065>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01745065>

CVE Reference: [CVE-2009-1418](#)

• CVE-2009-1671 Sun CVSS 2.0 Score = 9.3

Multiple buffer overflows in the Deployment Toolkit ActiveX control in deploytk.dll 6.0.130.3 in Sun Java SE Runtime Environment (aka JRE) 6 Update 13 allow remote attackers to execute arbitrary code via a long string argument to the (1) setInstallerType, (2) setAdditionalPackages, (3) compareVersion, (4) getStaticCLSID, or (5) launch method.

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

References:

MISC: http://www.shinnai.net/xplits/TXT_mhxRKrtrPLyAHRFNm7QR.html

BID: <http://www.securityfocus.com/bid/34931>

MILWORM: <http://www.milw0rm.com/exploits/8665>

CVE Reference: [CVE-2009-1671](#)

• **CVE-2009-1672 Sun CVSS 2.0 Score = 9.3**

The Deployment Toolkit ActiveX control in deploytk.dll 6.0.130.3 in Sun Java SE Runtime Environment (aka JRE) 6 Update 13 allows remote attackers to (1) execute arbitrary code via a .jnlp URL in the argument to the launch method, and might allow remote attackers to launch JRE installation processes via the (2) installLatestJRE or (3) installJRE method.

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

References:

MISC: http://www.shinnai.net/xplits/TXT_mhxRKrtrPLyAHRFNm7QR.html

BID: <http://www.securityfocus.com/bid/34931>

MILWORM: <http://www.milw0rm.com/exploits/8665>

CVE Reference: [CVE-2009-1672](#)

• **CVE-2009-1673 Sun CVSS 2.0 Score = 4.9**

The kernel in Sun Solaris 9 allows local users to cause a denial of service (panic) by calling fstat with a first argument of AT_FDCWD.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/1315>

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-66-257988-1>

CONFIRM: <http://sunsolve.sun.com/search/document.do?assetkey=1-21-122300-40-1>

BID: <http://www.securityfocus.com/bid/34979>

CVE Reference: [CVE-2009-1673](#)

• **CVE-2009-1656 Xerox CVSS 2.0 Score = 10.0**

Xerox WorkCentre and WorkCentre Pro 232, 238, 245, 255, 265, 275; and WorkCentre 5632, 5638, 5645, 5655, 5665, 5675, 5687, 7655, 7656, and 7675 allows remote attackers to execute arbitrary commands via unknown attack vectors, aka "command injection vulnerability."

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

References:

CONFIRM: http://www.xerox.com/downloads/usa/en/c/cert_XRX09-02_v1.0.pdf

VUPEN: <http://www.vupen.com/english/advisories/2009/1328>

SECUNIA: <http://secunia.com/advisories/35101>

CVE Reference: [CVE-2009-1656](#)

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