

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

[WinHoneyd v1.1.1](#) - Download WinHoneyd executable package by filling our download form. Size: 2384KB

Download Here:

<http://www.netvigilance.com/productdownloads?productname=winhoneyd-1.1.1.zip>

This Week in Review

Winner of Security Innovators Throwdown. New rule on net neutrality just the beginning. Large fine for data breach. China cyberspying.

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

• SC World Congress concludes with announcement of winners of Security Innovators Throwdown

The second annual SC World Congress conference and expo, the East Coast's largest security event, concluded with the announcement of the winners of its inaugural Security Innovators Throwdown, showcasing young companies, new technologies and groundbreaking services likely to impact the future information security landscape.

At the inaugural event, after presentations to a distinguished panel of experts, based on their vision and demonstrated ability to express the the viability of their technologies, the following companies were declared the top five innovators within the industry: Coming in at the top was HyTrust, which offers a tool for the control and visibility for a virtual infrastructure. At No. 2 was Yubico, with its hardware authentication token. Coming in third was Envision, which offers a software-as-a-service suite for CISOs to run their programs more effectively. Fourth was SMS Passcode, which makes two-factor authentication systems using mobile phone SMS. And fifth was SilverTail, which offers a solution for the detection of new fraudulent behavior on websites. SC Magazine

Full Story :

<http://www.scmagazineus.com/SC-World-Congress-concludes-with-announcement-of-winners-of-Security-Innovator>

• Net neutrality still faces political, legal hurdles

The FCC headquarters in Washington, D.C.

(Credit: FCC) Net neutrality supporters may be celebrating the Federal Communications Commission's unanimous vote Thursday to begin developing open Internet regulation, but the battle is far from over as the yet-to-be-written regulation is already facing Congressional opposition and will also likely be challenged in court.

Votes at the FCC for the proposal to get the ball rolling on new rules to protect an open Internet hadn't even been cast when Senator John McCain (R-Ariz.) introduced legislation on Thursday morning that would block the agency from regulating the Internet. McCain said that Net neutrality rules would stifle innovation and hurt the job market. Cnet Security

Full Story :

http://news.cnet.com/8301-30686_3-10381620-266.html?part=rss&subj=news&tag=2547-1_3-0-20

• **ChoicePoint to pay \$275,000 in latest data breach**

ChoicePoint, one of the nation's largest data brokers, has been fined \$275,000 by the U.S. Federal Trade Commission for a data breach that exposed personal information of 13,750 people last year.

In April 2008, ChoicePoint turned off a key electronic security tool that it used to monitor access to one of its databases and failed to notice the problem for four months, according to an FTC statement.

During that period, unauthorized searches were conducted for 30 days on a ChoicePoint database that contained Social Security numbers and other sensitive information, the FTC said. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-10379722-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• **Security report finds Chinese cyberspying threat growing**

A new report prepared for the U.S.-China Economic and Security Review Commission has concluded that the Asian nation is likely using his sophisticated IT systems to spy on America.

The report, released Thursday, analyzed China's information warfare strategy and offered up a case study in which an unnamed U.S. company was infiltrated by hackers to collect research-and-development information. Prepared by defense contractor Northrop Grumman, the report cited evidence that suggested the Chinese government endorsed that mission. SC Magazine

Full Story :

<http://www.scmagazineus.com/Security-report-finds-Chinese-cyberspying-threat-growing/article/156013/>

New Vulnerabilities Tested in SecureScout

• **18564 IIS FTP Service DoS Vulnerability (MS09-053/975254) (Remote File Checking)**

A vulnerability exists in the FTP Service in Microsoft Internet Information Services (IIS) 5.0, Microsoft Internet Information Services (IIS) 5.1, Microsoft Internet Information Services (IIS) 6.0, and Microsoft Internet Information Services (IIS) 7.0. The vulnerability could allow denial of service (DoS).

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

References:

* FULLDISC: 20090903 Microsoft Internet Information Services 5.0/6.0 FTP SERVER DENIAL OF SERVICE ("Stack Exhaustion")

<http://archives.neohapsis.com/archives/fulldisclosure/2009-09/0040.html>

* MS: MS09-053

<http://www.microsoft.com/technet/security/Bulletin/MS09-053.msp>

* BID: 36273

<http://www.securityfocus.com/bid/36273>

* VUPEN: VUPEN/ADV-2009-2542

<http://www.vupen.com/english/advisories/2009/2542>

* SECTRACK: 1022792

<http://securitytracker.com/alerts/2009/Aug/1022792.html>

* SECUNIA: SA36594

<http://secunia.com/advisories/36594/>

CVE Reference:

CVE-2009-2521 (cve.mitre.org, nvd.nist.gov)

• **18565 IIS FTP Service RCE and DoS Vulnerability (MS09-053/975254) (Remote File Checking)**

A Vulnerability exists in the FTP Service in Microsoft Internet Information Services (IIS) 5.0, Microsoft Internet Information Services (IIS) 5.1, and Microsoft Internet Information Services (IIS) 6.0. The vulnerability could allow remote code execution (RCE) on systems running FTP Service on IIS 5.0, or denial of service (DoS) on systems running FTP Service on IIS 5.1, IIS 6.0.

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

References:

- * MILWORM: 9541
<http://www.milw0rm.com/exploits/9541>
- * MILWORM: 9559
<http://www.milw0rm.com/exploits/9559>
- * MS: MS09-053
<http://www.microsoft.com/technet/security/Bulletin/MS09-053.msp>
- * BID: 36189
<http://www.securityfocus.com/bid/36189>
- * VUPEN: ADV-2009-2481
<http://www.vupen.com/english/advisories/2009/2481>
- * SECTRAK: 1022792
<http://securitytracker.com/alerts/2009/Aug/1022792.html>
- * SECUNIA: SA36594
<http://secunia.com/advisories/36594/>

CVE Reference:

CVE-2009-3023 (cve.mitre.org, nvd.nist.gov)

• 18566 Windows Media Runtime Voice Sample Rate Vulnerability (MS09-051/975682) (Remote File Checking)

A remote code execution vulnerability exists in Windows Media Player due to the improper processing of specially crafted Advanced Systems Format (ASF) files. An attacker could exploit the vulnerability by constructing a specially crafted audio file that could allow remote code execution when played using an affected version of Windows Media Player. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

- * MS: MS09-051
<http://www.microsoft.com/technet/security/Bulletin/MS09-051.msp>
- * BID: 36614
<http://www.securityfocus.com/bid/36614>
- * SECTRAK: 1023005
<http://securitytracker.com/alerts/2009/Oct/1023005.html>
- * VUPEN: VUPEN/ADV-2009-2887
<http://www.vupen.com/english/advisories/2009/2887>

CVE Reference:

CVE-2009-0555 (cve.mitre.org, nvd.nist.gov)

• 18567 Windows Media Runtime Heap Corruption Vulnerability (MS09-051/975682) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Windows Media Runtime handles certain functions in compressed audio files. This vulnerability could allow remote code execution if a user opened a specially crafted file. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

- * MS: MS09-051
<http://www.microsoft.com/technet/security/Bulletin/MS09-051.msp>
- * BID: 36602
<http://www.securityfocus.com/bid/36602>
- * SECTRAK: 1023005
<http://securitytracker.com/alerts/2009/Oct/1023005.html>
- * VUPEN: VUPEN/ADV-2009-2887

<http://www.vupen.com/english/advisories/2009/2887>

CVE Reference:

CVE-2009-2525 (cve.mitre.org, nvd.nist.gov)

• **18568 Windows Media Player Heap Overflow Vulnerability (MS09-052/974112) (Remote File Checking)**

A remote code execution vulnerability exists in Windows Media Player 6.4. An attacker could exploit the vulnerability by constructing a specially crafted ASF file that could allow remote code execution when played using Windows Media Player 6.4. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

* MS: MS09-052

<http://www.microsoft.com/technet/security/Bulletin/MS09-052.mspx>

* BID: 36644

<http://www.securityfocus.com/bid/36644>

* SECTRACK: 1023012

<http://securitytracker.com/alerts/2009/Oct/1023012.html>

* VUPEN: VUPEN/ADV-2009-2888

<http://www.vupen.com/english/advisories/2009/2888>

CVE Reference:

CVE-2009-2527 (cve.mitre.org, nvd.nist.gov)

• **18569 Null Truncation in X.509 Common Name Vulnerability (MS09-056/974571) (Remote File Checking)**

A spoofing vulnerability exists in the Microsoft Windows CryptoAPI component when parsing ASN.1 information from X.509 certificates. An attacker who successfully exploited this vulnerability could impersonate another user or system.

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

References:

* MS: MS09-056

<http://www.microsoft.com/technet/security/Bulletin/MS09-056.mspx>

* BID: 36475

<http://www.securityfocus.com/bid/36475>

* SECTRACK: 1023013

<http://securitytracker.com/alerts/2009/Oct/1023013.html>

* VUPEN: VUPEN/ADV-2009-2891

<http://www.vupen.com/english/advisories/2009/2891>

CVE Reference:

CVE-2009-2510 (cve.mitre.org, nvd.nist.gov)

• **18570 Integer Overflow in X.509 Object Identifiers Vulnerability (MS09-056/974571) (Remote File Checking)**

A spoofing vulnerability exists in the Microsoft Windows CryptoAPI component when parsing ASN.1 object identifiers from X.509 certificates. An attacker who successfully exploited this vulnerability could impersonate another user or system.

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

References:

* MS: MS09-056

<http://www.microsoft.com/technet/security/Bulletin/MS09-056.mspx>

* BID: 36577

<http://www.securityfocus.com/bid/36577>

* SECTRACK: 1023013

<http://securitytracker.com/alerts/2009/Oct/1023013.html>

* VUPEN: VUPEN/ADV-2009-2891

<http://www.vupen.com/english/advisories/2009/2891>

CVE Reference:

CVE-2009-2511 (cve.mitre.org, nvd.nist.gov)

• 18571 ATL Uninitialized Object Vulnerability (MS09-060/973965) (Remote File Checking)

A remote code execution vulnerability exists in the Microsoft Active Template Library (ATL) due to an issue in the ATL headers that could allow an attacker to force VariantClear to be called on a VARIANT that has not been correctly initialized. Because of this, the attacker can control what happens when VariantClear is called during handling of an error by supplying a corrupt stream. This vulnerability only directly affects systems with components and controls installed that were built using Visual Studio ATL. This issue could allow a remote, unauthenticated user to perform remote code execution on an affected system. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution.

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

References:

- * MS: MS09-060
<http://www.microsoft.com/technet/security/Bulletin/MS09-060.msp>
- * BID: 35832
<http://www.securityfocus.com/bid/35832>
- * SECTRACK: 1022610
<http://securitytracker.com/alerts/2009/Jul/1022610.html>
- * VUPEN: VUPEN/ADV-2009-2895
<http://www.vupen.com/english/advisories/2009/2895>

CVE Reference:

CVE-2009-0901 (cve.mitre.org, nvd.nist.gov)

• 18572 ATL COM Initialization Vulnerability (MS09-060/973965) (Remote File Checking)

A remote code execution vulnerability exists in the Microsoft Active Template Library (ATL) due to issues in the ATL headers that handle instantiation of an object from data streams. This vulnerability only directly affects systems with components and controls installed that were built using Visual Studio ATL. For components and controls built using ATL, unsafe usage of OleLoadFromStream could allow the instantiation of arbitrary objects which can bypass related security policy, such as kill bits within Internet Explorer. This issue could allow a remote, unauthenticated user to perform remote code execution on an affected system. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution.

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

References:

- * MS: MS09-060
<http://www.microsoft.com/technet/security/Bulletin/MS09-060.msp>
- * BID: 35828
<http://www.securityfocus.com/bid/35828>
- * SECTRACK: 1022610
<http://securitytracker.com/alerts/2009/Jul/1022610.html>
- * VUPEN: VUPEN/ADV-2009-2895
<http://www.vupen.com/english/advisories/2009/2895>

CVE Reference:

CVE-2009-2493 (cve.mitre.org, nvd.nist.gov)

• 18573 ATL Null String Vulnerability (MS09-060/973965) (Remote File Checking)

An information disclosure vulnerability exists in the Microsoft Active Template Library (ATL) that could allow a string to be read without a terminating NULL character. An attacker could manipulate this string to read extra data beyond the end of the string and thus disclose information in memory. This vulnerability only directly affects systems with components and controls installed that were built using Visual Studio ATL. An attacker who successfully exploited this vulnerability could run a malicious component or control that could disclose information, forward user data to a third party, or access any data on the affected systems that was accessible to the logged-on user. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly, but it could be used to produce information that could be used to try to further compromise the affected system.

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

References:

- * MS: MS09-060
<http://www.microsoft.com/technet/security/Bulletin/MS09-060.msp>
- * BID: 35830
<http://www.securityfocus.com/bid/35830>
- * SECTRACK: 1022610

<http://securitytracker.com/alerts/2009/Jul/1022610.html>

* VUPEN: VUPEN/ADV-2009-2895

<http://www.vupen.com/english/advisories/2009/2895>

CVE Reference:

CVE-2009-2495 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-1979 Oracle CVSS 2.0 Score = 10.0

Unspecified vulnerability in the Network Authentication component in Oracle Database 10.1.0.5 and 10.2.0.4 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/cpuoct2009.html>

CVE Reference: [CVE-2009-1979](http://cve.mitre.org/cve/2009/1979)

• CVE-2009-1985 Oracle CVSS 2.0 Score = 10.0

Unspecified vulnerability in the Network Authentication component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, and 10.2.0.4 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/cpuoct2009.html>

CVE Reference: [CVE-2009-1985](http://cve.mitre.org/cve/2009/1985)

• CVE-2009-1992 Oracle CVSS 2.0 Score = 10.0

Unspecified vulnerability in the Core RDBMS component in Oracle Database 9.2.0.8, 10.1.0.5, and 10.2.0.4 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/cpuoct2009.html>

CVE Reference: [CVE-2009-1992](http://cve.mitre.org/cve/2009/1992)

• CVE-2009-3403 Oracle CVSS 2.0 Score = 10.0

Unspecified vulnerability in the JRockit component in BEA Product Suite R27.6.4: JRE/JDK, 1.4.2, 5, and, and 6 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors. NOTE: this issue subsumes CVE-2009-2670, CVE-2009-2671, CVE-2009-2672, CVE-2009-2673, CVE-2009-2674, CVE-2009-2675, and CVE-2009-2676.

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

References:

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html>

CVE Reference: [CVE-2009-3403](http://cve.mitre.org/cve/2009/3403)

• CVE-2009-1007 Oracle CVSS 2.0 Score = 6.5

Unspecified vulnerability in the Data Mining component in Oracle Database 10.2.0.4 allows remote authenticated users to affect confidentiality, integrity, and availability, related to SYS.DMP_SYS.

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

References:

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html>

CVE Reference: [CVE-2009-1007](http://cve.mitre.org/cve/2009/1007)

• **CVE-2009-1994 Oracle CVSS 2.0 Score = 6.5**

Unspecified vulnerability in the Oracle Spatial component in Oracle Database 10.1.0.5 allows remote authenticated users to affect confidentiality, integrity, and availability, related to MDSYS.PRVT_CMT_CBK.

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

References:

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html>

CVE Reference: [CVE-2009-1994](#)

• **CVE-2009-2001 Oracle CVSS 2.0 Score = 6.5**

Unspecified vulnerability in the PL/SQL component in Oracle Database 10.2.0.4 and 11.1.0.7 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors.

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

References:

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html>

CVE Reference: [CVE-2009-2001](#)

• **CVE-2009-1018 Oracle CVSS 2.0 Score = 5.5**

Unspecified vulnerability in the Workspace Manager component in Oracle Database 10.2.0.4 allows remote authenticated users to affect confidentiality and integrity, related to SYS.LTRIC (WMSYS.LTRIC).

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

References:

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html>

CVE Reference: [CVE-2009-1018](#)

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