

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 v1.5c](#) - Download WinHoneyd executable package by filling our download form. Size: 2407KB

Download Here:

<http://www.netvigilance.com/productdownloads?productname=winhoneyd-1.5c.zip>

This Week in Review

Obama's cybersecurity plan under criticism. Pirate site hides malware. Enterprise security today. Will new White House cybersecurity negative impact Homeland cybersecurity?

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

• Experts: Obama cybersecurity plan short on details

IDG News Service - U.S. President Barack Obama's new cybersecurity report is short on details and creates a federal coordinator position that may have limited power, some cybersecurity experts said Monday.

"That is not an indication that this office will be given large amounts of authority," said Baker, who served at DHS during former President George Bush's administration.

The report, released Friday, calls for the U.S. government to develop a national cybersecurity strategy in addition to the appointment of a federal cybersecurity coordinator. Obama also said cybersecurity would become a key management priority at the White House, and the report recommends a new cybersecurity incident response plan that involves both the U.S. government and the private sector.

Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9133773>

• **Software crack site hides malware repository**

A website found by a security research organization serves malicious files to people who are looking for cracks to software applications.

When a user clicks on a program in the list of supposedly pirated software, they get a download link that in the background transfers a .zip file containing two files, both of which are malicious trojans.

The .zip file is actually hosted on another domain, where more trouble awaits.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Software-crack-site-hides-malware-repository/article/137887/>

• **It's the Information, Stupid**

CSO - Over the past several years there have been changes in the business environment, causing fundamental alterations in how security organizations operate to protect the enterprises for which they have responsibility.

The focus of this article is to identify ways that information in the enterprise can be inappropriately removed and a framework for how to mitigate these risks and protect your organization from the potential litigation, fines, and sheer embarrassment that can follow from such an event. [See also: Seven Practical Ideas for Security Awareness]

Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9133909>

• **Lawmakers question whether DHS cybersecurity role will be undercut by White House appointment**

Computerworld - Just days after President Obama announced his plan to appoint a new White House cybersecurity coordinator, lawmakers are questioning the impact the move might have on the U.S. Department of Homeland Security's role in cybersecurity.

Sen. Susan Collins (R-Maine), a ranking member of the Senate Committee, said she had a "lot of reservations about the establishment of a White House cybersecurity czar." Such an appointment would make it far more difficult for members of Congress to provide oversight because it would not be easy to get a presidential adviser to testify before the committee, she said.

Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9133992>

New Vulnerabilities Tested in SecureScout

• **18395 QuickTime handling of Sorenson 3 video files, arbitrary code execution (Remote File Checking)**

A memory corruption issue exists in QuickTime's handling of Sorenson 3 video files. This may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.6.2.

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

References:

* MISC:

http://secunia.com/secunia_research/2009-10/

* CONFIRM:

<http://support.apple.com/kb/HT3591>

* APPLE: APPLE-SA-2009-06-01-1

<http://lists.apple.com/archives/security-announce/2009/Jun/msg00000.html>

* BID: 35159

<http://www.securityfocus.com/bid/35159>

* SECUNIA: 35091

<http://secunia.com/advisories/35091>

* VUPEN: ADV-2009-1469

<http://www.vupen.com/english/advisories/2009/1469>

CVE Reference:

CVE-2009-0188 (cve.mitre.org, nvd.nist.gov)

• 18396 QuickTime handling of FLC compression files, arbitrary code execution (Remote File Checking)

A heap buffer overflow exists in the handling of FLC compression files. Opening a maliciously crafted FLC compression file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.6.2.

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

References:

* CONFIRM:

<http://support.apple.com/kb/HT3591>

* APPLE: APPLE-SA-2009-06-01-1

<http://lists.apple.com/archives/security-announce/2009/Jun/msg00000.html>

* BID: 35161

<http://www.securityfocus.com/bid/35161>

* SECUNIA: 35091

<http://secunia.com/advisories/35091>

* VUPEN: ADV-2009-1469

<http://www.vupen.com/english/advisories/2009/1469>

CVE Reference:

CVE-2009-0951 (cve.mitre.org, nvd.nist.gov)

• 18397 QuickTime processing a compressed PSD image, arbitrary code execution (Remote File Checking)

A buffer overflow may occur while processing a compressed PSD image. Opening a maliciously crafted compressed PSD file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.6.2.

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

References:

* CONFIRM:

<http://support.apple.com/kb/HT3591>

* APPLE: APPLE-SA-2009-06-01-1

<http://lists.apple.com/archives/security-announce/2009/Jun/msg00000.html>

* BID: 35168

<http://www.securityfocus.com/bid/35168>

* SECUNIA: 35091

<http://secunia.com/advisories/35091>

* VUPEN: ADV-2009-1469

<http://www.vupen.com/english/advisories/2009/1469>

CVE Reference:

CVE-2009-0952 (cve.mitre.org, nvd.nist.gov)

• 18398 QuickTime handling of PICT images, arbitrary code execution (Remote File Checking)

An integer underflow in QuickTime's handling of PICT images may result in a heap buffer overflow. Opening a maliciously crafted PICT file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.6.2.

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

References:

* BUGTRAQ: 20090527 ZDI-09-021: Apple QuickTime PICT Unspecified Tag Heap Overflow Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/503878/100/0/threaded>

* MISC:

[http://www.vupen.com/exploits/Apple QuickTime PICT Poly Tag Parsing Heap Overflow PoC Exploit 1407144.php](http://www.vupen.com/exploits/Apple_QuickTime_PICT_Poly_Tag_Parsing_Heap_Overflow_PoC_Exploit_1407144.php)

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-09-021/>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-09-021>

* CONFIRM:

<http://support.apple.com/kb/HT3549>

* CONFIRM:

<http://support.apple.com/kb/HT3591>

* APPLE: APPLE-SA-2009-05-12

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

* APPLE: APPLE-SA-2009-06-01-1

<http://lists.apple.com/archives/security-announce/2009/Jun/msg00000.html>

* CERT: TA09-133A

<http://www.us-cert.gov/cas/techalerts/TA09-133A.html>

* BID: 34926

<http://www.securityfocus.com/bid/34926>

* BID: 34938

<http://www.securityfocus.com/bid/34938>

* SECTRACK: 1022209

<http://www.securitytracker.com/id?1022209>

* SECUNIA: 35074

<http://secunia.com/advisories/35074>

* SECUNIA: 35091

<http://secunia.com/advisories/35091>

* VUPEN: ADV-2009-1297

<http://www.vupen.com/english/advisories/2009/1297>

* VUPEN: ADV-2009-1407

<http://www.vupen.com/english/advisories/2009/1407>

CVE Reference:

CVE-2009-0010 (cve.mitre.org, nvd.nist.gov)

• 18399 QuickTime handling of PICT images, arbitrary code execution (CVE-2009-0953) (Remote File Checking)

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

The issue has been fixed in version 7.6.2.

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

References:

* CONFIRM:

<http://support.apple.com/kb/HT3591>

* APPLE: APPLE-SA-2009-06-01-1

<http://lists.apple.com/archives/security-announce/2009/Jun/msg00000.html>

* BID: 35164

<http://www.securityfocus.com/bid/35164>

* SECUNIA: 35091

<http://secunia.com/advisories/35091>

* VUPEN: ADV-2009-1469

<http://www.vupen.com/english/advisories/2009/1469>

CVE Reference:

CVE-2009-0953 (cve.mitre.org, nvd.nist.gov)

• 18400 QuickTime handling of Clipping Region (CRGN) atom types in a movie file, arbitrary code execution (Remote File Checking)

A heap buffer overflow exists in QuickTime's handling of Clipping Region (CRGN) atom types in a movie file. Opening a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.6.2.

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

References:

* CONFIRM:

<http://support.apple.com/kb/HT3591>

* APPLE: APPLE-SA-2009-06-01-1

<http://lists.apple.com/archives/security-announce/2009/Jun/msg00000.html>

* BID: 35167

<http://www.securityfocus.com/bid/35167>

* SECUNIA: 35091

<http://secunia.com/advisories/35091>

* VUPEN: ADV-2009-1469

<http://www.vupen.com/english/advisories/2009/1469>

CVE Reference:

CVE-2009-0954 (cve.mitre.org, nvd.nist.gov)

• 18401 QuickTime handling of MS ADPCM encoded audio data, arbitrary code execution (Remote File Checking)

A heap buffer overflow exists in the handling of MS ADPCM encoded audio data. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.6.2.

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

References:

* MISC:

http://secunia.com/secunia_research/2009-6/

* CONFIRM:

<http://support.apple.com/kb/HT3591>

* APPLE: APPLE-SA-2009-06-01-1

<http://lists.apple.com/archives/security-announce/2009/Jun/msg00000.html>

* BID: 35163

<http://www.securityfocus.com/bid/35163>

* SECUNIA: 35091

<http://secunia.com/advisories/35091>

* VUPEN: ADV-2009-1469

<http://www.vupen.com/english/advisories/2009/1469>

CVE Reference:

CVE-2009-0185 (cve.mitre.org, nvd.nist.gov)

• 18402 QuickTime handling of image description atoms, arbitrary code execution (Remote File Checking)

A sign extension issue exists in QuickTime's handling of image description atoms. Opening a maliciously crafted Apple video file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.6.2.

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

References:

* CONFIRM:

<http://support.apple.com/kb/HT3591>

* APPLE: APPLE-SA-2009-06-01-1

<http://lists.apple.com/archives/security-announce/2009/Jun/msg00000.html>

* BID: 35166

<http://www.securityfocus.com/bid/35166>

* SECUNIA: 35091

<http://secunia.com/advisories/35091>

* VUPEN: ADV-2009-1469

<http://www.vupen.com/english/advisories/2009/1469>

CVE Reference:

CVE-2009-0955 (cve.mitre.org, nvd.nist.gov)

• 18403 QuickTime handling of movie files, arbitrary code execution (Remote File Checking)

An uninitialized memory access issue exists in QuickTime's handling of movie files. Viewing a movie file with a zero user data atom size may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.6.2.

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

References:

- * CONFIRM:
<http://support.apple.com/kb/HT3591>
- * APPLE: APPLE-SA-2009-06-01-1
<http://lists.apple.com/archives/security-announce/2009/Jun/msg00000.html>
- * BID: 35162
<http://www.securityfocus.com/bid/35162>
- * SECUNIA: 35091
<http://secunia.com/advisories/35091>
- * VUPEN: ADV-2009-1469
<http://www.vupen.com/english/advisories/2009/1469>

CVE Reference:

CVE-2009-0956 (cve.mitre.org, nvd.nist.gov)

• 18404 QuickTime handling of JP2 images, arbitrary code execution (Remote File Checking)

A heap buffer overflow exists in QuickTime's handling of JP2 images. Viewing a maliciously crafted JP2 image may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.6.2.

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

References:

- * CONFIRM:
<http://support.apple.com/kb/HT3591>
- * APPLE: APPLE-SA-2009-06-01-1
<http://lists.apple.com/archives/security-announce/2009/Jun/msg00000.html>
- * BID: 35165
<http://www.securityfocus.com/bid/35165>
- * SECUNIA: 35091
<http://secunia.com/advisories/35091>
- * VUPEN: ADV-2009-1469
<http://www.vupen.com/english/advisories/2009/1469>

CVE Reference:

CVE-2009-0957 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-6819 Microsoft CVSS 2.0 Score = 4.7

win32k.sys in Microsoft Windows Server 2003 and Vista allows local users to cause a denial of service (system crash) via vectors related to CreateWindow, TranslateMessage, and DispatchMessage, possibly a race condition between threads, a different vulnerability than CVE-2008-1084. NOTE: some of these details are obtained from third party information.

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

References:

- MISC: <http://www.securityfocus.com/data/vulnerabilities/exploits/35121.c>
- BID: <http://www.securityfocus.com/bid/35121>
- MISC: <http://bugtraq.ru/cgi-bin/forum.mcgi?type=sb&b=2&m=152274>

CVE Reference: [CVE-2008-6819](http://cve.mitre.org)

• CVE-2009-0896 IBM CVSS 2.0 Score = 10.0

Buffer overflow in the queue manager in IBM WebSphere MQ 6.x before 6.0.2.7 and 7.x before 7.0.1.0 allows remote attackers to execute arbitrary code via a crafted request.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/1463>
CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21386826>
XF: <http://xforce.iss.net/xforce/xfdb/50641>
BID: <http://www.securityfocus.com/bid/35170>
AIXAPAR: <http://www-1.ibm.com/support/docview.wss?uid=swg1Iz50784>
SECTRAK: <http://securitytracker.com/id?1022311>
SECUNIA: <http://secunia.com/advisories/35303>

CVE Reference: [CVE-2009-0896](#)

• **CVE-2008-6820 IBM CVSS 2.0 Score = 10.0**

The db2fmp process in IBM DB2 8 before FP17, 9.1 before FP5, and 9.5 before FP2 on Windows runs with "OS privilege," which has unknown impact and attack vectors, a different vulnerability than CVE-2008-3856.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21318189>
AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1JR30228>
AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1JR30227>
AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1JR30026>
CONFIRM: ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2_v82/APARLIST.TXT

CVE Reference: [CVE-2008-6820](#)

• **CVE-2008-6821 IBM CVSS 2.0 Score = 10.0**

Buffer overflow in the DAS server in IBM DB2 8 before FP17, 9.1 before FP5, and 9.5 before FP2 might allow attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors, a different vulnerability than CVE-2007-3676 and CVE-2008-3853.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21318189>
AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1Iz22190>
AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1Iz22188>
AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1Iz22004>
CONFIRM: ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2_v82/APARLIST.TXT
SECUNIA: <http://secunia.com/advisories/31787>

CVE Reference: [CVE-2008-6821](#)

• **CVE-2009-1899 IBM CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the System Management/Repository component in IBM WebSphere Application Server (WAS) 6.0.2 before 6.0.2.35 has unknown impact and attack vectors, related to a "security exposure in wsadmin."

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/1464>

AIXAPAR: <http://www-1.ibm.com/support/docview.wss?uid=swg1PK77495>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27006876>

SECUNIA: <http://secunia.com/advisories/35301>

CVE Reference: [CVE-2009-1899](#)

• **CVE-2009-1901 IBM CVSS 2.0 Score = 7.5**

The Security component in IBM WebSphere Application Server (WAS) 6.0.2 before 6.0.2.35 permits "non-standard http methods," which has unknown impact and remote attack vectors.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/1464>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27006876>

AIXAPAR: <http://www-1.ibm.com/support/docview.wss?uid=swg1PK73246>

CVE Reference: [CVE-2009-1901](#)

• **CVE-2009-1898 IBM CVSS 2.0 Score = 5.0**

The secure login page in the Administrative Console component in IBM WebSphere Application Server (WAS) 6.0.2 before 6.0.2.35 does not redirect to an https page upon receiving an http request, which makes it easier for remote attackers to read the contents of WAS sessions by sniffing the network.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/1464>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27006876>

AIXAPAR: <http://www-1.ibm.com/support/docview.wss?uid=swg1PK77010>

SECUNIA: <http://secunia.com/advisories/35301>

CVE Reference: [CVE-2009-1898](#)

• **CVE-2009-1900 IBM CVSS 2.0 Score = 5.0**

The Configservice APIs in the Administrative Console component in IBM WebSphere Application Server (WAS) 6.0.2 before 6.0.2.35 allow attackers to obtain sensitive information via unspecified vectors.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/1464>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27006876>

AIXAPAR: <http://www-1.ibm.com/support/docview.wss?uid=swg1PK84999>

SECUNIA: <http://secunia.com/advisories/35301>

CVE Reference: [CVE-2009-1900](#)

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