

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

Privacy redefined. A story from real life. Recession puts corporate data at risk. Newly formed group to better encryption standard.

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

• Fixing the privacy joke

February 9, 2009 (Network World) The whole idea of privacy has become a joke. On one hand we have consumers who will give away their personal details to random Web sites (as well as to Mrs. Sikiratu Seki Adam, "a widow to Late Saheed Baba Adams") at the drop of a virtual hat, and on the other we have businesses losing personally identifiable information and transaction data with wild abandon ... yes, I'm talking about you Heartland Payment Systems. (Heartland lost data on more than 100 million transactions although it is hardly alone -- check out the data loss database at the Open Security Foundation).

What got me thinking about this privacy void was a letter my wife received from Nordstrom Bank yesterday. My wife has a Nordstrom credit card and the company sent us, for what seems like the 1,000th time, its latest privacy policy.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127611&source=rss_topic1

• Fight Back Against Cybersquatters

February 10, 2009 (PC World) The story you are about to read is true. The names have been changed to protect the pond scum who hijacked the name of a not-for-profit animal rescue group. Not that they deserve protection.

The group is redoing its Web site, and I asked whether I'd find it at petrescueofcarbona.org, the logical name for such a group. "No," I was told, "we have dot u-s for our domain." (Disclaimer: I am not an officer or spokesperson for the group).

Running a WHOIS on the domain failed to turn up an owner for it, so I opened the browser and typed in the domain URL.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127705&source=rss_topic1

• Recession raises threat of data walking out the door

February 11, 2009 (Network World) Moving into 2009, the number of layoffs and unemployed has multiplied as a result of the falling economy. Corporate data is at risk now more than ever and companies need to be sure they have reliable protection in place.

Employees can confiscate sensitive company data by saving it to a memory stick, e-mailing it to a personal account, or even walking out with a laptop or BlackBerry. Companies need to be protected in all instances to ensure their information doesn't walk out the door.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127788&source=rss_topic1

• HP, IBM push new OASIS encryption key standard

February 12, 2009 (IDG News Service) A group of industry vendors, led by IBM, Hewlett-Packard and EMC, is proposing a new standard to make their encryption management software work together.

On Thursday, OASIS is expected to announce that it has created a KMIP Technology Committee to produce the final specification for the standard. The committee will meet for the first time on April 24, but KMIP has been quietly under development for more than a year. It is also supported by Brocade, LSI, Seagate and Thales.

KMIP's backers say their standard will be "complementary" to existing key management standards such as the storage-focused IEEE 1619.3 and the OASIS EKMI XML standard.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127843&source=rss_topic1

New Vulnerabilities Tested in SecureScout

• 16705 Oracle Enterprise Manager - Enterprise Manager Console component unspecified Vulnerability (jan-2007/EM04)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html>

* CERT: TA07-017A

<http://www.us-cert.gov/cas/techalerts/TA07-017A.html>

* SECTRACK: 1017522

<http://securitytracker.com/id?1017522>

* SECUNIA: 23794

<http://secunia.com/advisories/23794>

* XF: oracle-cpu-jan2007(31541)

<http://xforce.iss.net/xforce/xfdb/31541>

CVE Reference:

CVE-2007-0293 (cve.mitre.org, nvd.nist.gov)

• 16706 Oracle Enterprise Manager - Enterprise Manager Console component unspecified Vulnerability (jan-2007/EM05)

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

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html>
- * CERT: TA07-017A
<http://www.us-cert.gov/cas/techalerts/TA07-017A.html>
- * SECTRACK: 1017522
<http://securitytracker.com/id?1017522>
- * SECUNIA: 23794
<http://secunia.com/advisories/23794>
- * XF: oracle-cpu-jan2007(31541)
<http://xforce.iss.net/xforce/xfdb/31541>

CVE Reference:

CVE-2007-0293 (cve.mitre.org, nvd.nist.gov)
CVE-2007-0292 (cve.mitre.org, nvd.nist.gov)

• 16707 Oracle Enterprise Manager - Database Cloning & Data Guard Management component unspecified Vulnerability (jan-2007/EM06)

An unspecified vulnerability with unknown impact exists in Oracle Enterprise Manager Database Cloning & Data Guard Management component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html>
- * CERT: TA07-017A
<http://www.us-cert.gov/cas/techalerts/TA07-017A.html>
- * SECTRACK: 1017522
<http://securitytracker.com/id?1017522>
- * SECUNIA: 23794
<http://secunia.com/advisories/23794>
- * XF: oracle-cpu-jan2007(31541)
<http://xforce.iss.net/xforce/xfdb/31541>

CVE Reference:

CVE-2007-0294 (cve.mitre.org, nvd.nist.gov)

• 18262 Internet Explorer Uninitialized Memory Corruption Vulnerability (MS09-002/961260) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer accesses an object that has been deleted. 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. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user.

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

References:

- * MS: MS09-002
<http://www.microsoft.com/technet/security/Bulletin/MS09-002.mspx>
- * MISC: ZDI-09-011
<http://www.zerodayinitiative.com/advisories/ZDI-09-011/>
- * SECTRACK: 1021699
<http://securitytracker.com/alerts/2009/Feb/1021699.html>
- * BID: 33627
<http://www.securityfocus.com/bid/33627>

CVE Reference:

CVE-2009-0075 (cve.mitre.org, nvd.nist.gov)

• 18263 Internet Explorer CSS Memory Corruption Vulnerability (MS09-002/961260) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer handles Cascading Style Sheets (CSS). 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. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

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

References:

- * MS: MS09-002
<http://www.microsoft.com/technet/security/Bulletin/MS09-002.mspx>
- * MISC: ZDI-09-012
<http://www.zerodayinitiative.com/advisories/ZDI-09-012/>
- * SECTRACK: 1021699
<http://securitytracker.com/alerts/2009/Feb/1021699.html>
- * BID: 33628
<http://www.securityfocus.com/bid/33628>

CVE Reference:

CVE-2009-0076 (cve.mitre.org, nvd.nist.gov)

• 18264 Microsoft Exchange Server Memory Corruption Vulnerability (MS09-003/959239) (Remote File Checking)

A remote code execution vulnerability exists in the way Microsoft Exchange Server decodes the Transport Neutral Encapsulation Format (TNEF) data for a message.

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

References:

- * MS: MS09-003
<http://www.microsoft.com/technet/security/Bulletin/MS09-003.mspx>
- * BID: 33134
<http://www.securityfocus.com/bid/33134>
- * SECTRACK: 1021700
<http://securitytracker.com/alerts/2009/Feb/1021700.html>

CVE Reference:

CVE-2009-0098 (cve.mitre.org, nvd.nist.gov)

• 18265 Microsoft Exchange Server Literal Processing Vulnerability (MS09-003/959239) (Remote File Checking)

A denial of service vulnerability exists in the EMSMDB2 (Electronic Messaging System Microsoft Data Base, 32 bit build) provider because of the way it handles invalid MAPI commands. An attacker could exploit the vulnerability by sending a specially crafted MAPI command to the application using the EMSMDB32 provider. An attacker who successfully exploited this vulnerability could cause the application to stop responding.

The denial of service vulnerability also affects the Microsoft Exchange System Attendant since it uses the EMSMDB32 provider. The Microsoft Exchange System Attendant is one of the core services in Microsoft Exchange and performs a variety of functions related to the on-going maintenance of the Exchange system.

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

References:

- * MS: MS09-003
<http://www.microsoft.com/technet/security/Bulletin/MS09-003.mspx>
- * SECTRACK: 1021701
<http://securitytracker.com/alerts/2009/Feb/1021701.html>
- * BID: 33136
<http://www.securityfocus.com/bid/33136>

CVE Reference:

CVE-2009-0099 (cve.mitre.org, nvd.nist.gov)

● **18267 Microsoft Office Visio Memory Validation Vulnerability (CVE-2009-0095) (MS09-005/957634) (Remote File Checking)**

A remote code execution vulnerability exists in the way Microsoft Office Visio validates object data when opening up Visio files. An attacker could exploit the vulnerability by sending a specially crafted file which could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

If a user were 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 affected than users who operate with administrative user rights.

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

References:

* MS: MS09-005

<http://www.microsoft.com/technet/security/Bulletin/MS09-005.mspx>

* BID: 33659

<http://www.securityfocus.com/bid/33659>

CVE Reference:

CVE-2009-0095 (cve.mitre.org, nvd.nist.gov)

● **18268 Microsoft Office Visio Memory Validation Vulnerability (CVE-2009-0096) (MS09-005/957634) (Remote File Checking)**

A remote code execution vulnerability exists in the way Microsoft Office Visio copies object data in memory. An attacker could exploit the vulnerability by sending a malformed file which could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

If a user were 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 affected than users who operate with administrative user rights.

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

References:

* MS: MS09-005

<http://www.microsoft.com/technet/security/Bulletin/MS09-005.mspx>

* BID: 33660

<http://www.securityfocus.com/bid/33660>

CVE Reference:

CVE-2009-0096 (cve.mitre.org, nvd.nist.gov)

● **18269 Microsoft Office Visio Memory Validation Vulnerability (CVE-2009-0097) (MS09-005/957634) (Remote File Checking)**

A remote code execution vulnerability exists in the way Microsoft Office Visio handles memory when opening up Visio files. An attacker could exploit the vulnerability by sending a specially crafted file which could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

If a user were 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 affected than users who operate with administrative user rights.

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

References:

* MS: MS09-005

<http://www.microsoft.com/technet/security/Bulletin/MS09-005.mspx>

* BID: 33661

<http://www.securityfocus.com/bid/33661>

CVE Reference:

CVE-2009-0097 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2009-0076 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 7, when XHTML strict mode is used, allows remote attackers to execute arbitrary code via the zoom style directive in conjunction with unspecified other directives in a malformed Cascading Style Sheets (CSS) stylesheet in a crafted HTML document, aka "CSS Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-002.msp>

CVE Reference: [CVE-2009-0076](#)

- **CVE-2009-0095 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office Visio 2002 SP2, 2003 SP3, and 2007 SP1 does not properly validate object data in Visio files, which allows remote attackers to execute arbitrary code via a crafted file, aka "Memory Validation Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-005.msp>

CVE Reference: [CVE-2009-0095](#)

- **CVE-2009-0096 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office Visio 2002 SP2, 2003 SP3, and 2007 SP1 does not properly perform memory copy operations for object data, which allows remote attackers to execute arbitrary code via a crafted Visio document, aka "Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-005.msp>

CVE Reference: [CVE-2009-0096](#)

- **CVE-2009-0097 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office Visio 2002 SP2 and 2003 SP3 does not properly validate memory allocation for Visio files, which allows remote attackers to execute arbitrary code via a crafted file, aka "Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-005.msp>

CVE Reference: [CVE-2009-0097](#)

- **CVE-2009-0098 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Exchange 2000 Server SP3, Exchange Server 2003 SP2, and Exchange Server 2007 SP1 do not properly interpret Transport Neutral Encapsulation (TNEF) properties, which allows remote attackers to execute arbitrary code via a crafted TNEF message, aka "Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-003.msp>

CVE Reference: [CVE-2009-0098](#)

- **CVE-2009-0075 Microsoft CVSS 2.0 Score = 8.5**

Microsoft Internet Explorer 7 does not properly handle errors during attempted access to deleted objects, which allows remote attackers to execute arbitrary code via a crafted HTML document, related to CFunctionPointer and the appending of document objects, aka "Uninitialized Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-002.msp>

CVE Reference: [CVE-2009-0075](#)

• **CVE-2009-0099 Microsoft CVSS 2.0 Score = 5.0**

The Electronic Messaging System Microsoft Data Base (EMSMDB32) provider in Microsoft Exchange 2000 Server SP3 and Exchange Server 2003 SP2, as used in Exchange System Attendant, allows remote attackers to cause a denial of service (application outage) via a malformed MAPI command, aka "Literal Processing Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-003.msp>

CVE Reference: [CVE-2009-0099](#)

• **CVE-2008-4559 HP CVSS 2.0 Score = 10.0**

HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via shell metacharacters in argument fields to the (1) webappmon.exe or (2) OpenView5.exe CGI program. NOTE: this issue may be partially covered by CVE-2009-0205.

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

References:

IDEFENSE: <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=770>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01661610>

CVE Reference: [CVE-2008-4559](#)

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