ScoutNews
The weekly Security update from the makers of SecureScout
October 16, 2009

2009 Issue #42

Table of Contents

Product Focus

WinHoneyd v1.5b - Download WinHoneyd executable package by filling our download form. Size: 2404KB

Download Here:
http://www.netvigilance.com/productdownloads?productname=winhoneyd-1.5b.zip

This Week in Review

FBI Cyber Division successful. Employees key to data security. How to get your message through. New way of detecting malware.

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: Feds talk cybersecurity**

Top officials from U.S. law enforcement and government agencies speaking at SC World Congress in New York this week said progress has been made in fighting cybercrime recently, but increased collaboration with individuals from the private sector and international law enforcement bodies is needed to keep up the momentum.

Shawn Henry, assistant director of the FBI Cyber Division, said that efforts to cooperate with foreign law enforcement agencies have paid off in the fight against cybercriminals. Six years ago, for example, the FBI could not respond to an attack that was traced back to an individual outside of the U.S, Henry said. Today, FBI agents are working hand-in-hand with international law enforcement agents in Estonia, Romania and other countries to build cases against cybercriminals and make arrests. SC Magazine

Full Story :
http://www.scmagazineus.com/SC-World-Congress-Feds-talk-cybersecurity/article/152294/

- **SC World Congress: Worker training key to data protection**

An effective security awareness campaign doesn't make security experts out of company employees. It just makes them know who to call in case something happens.

That was the message from Dow Williamson, executive director of SCIPP International, which provides security awareness training and certification programs for organizations worldwide. Williamson spoke Tuesday on a panel with Kris Rowely, CISO of the state of Vermont, at the second annual SC World Congress in New York.

Williamson emphasized the importance of end-user training, saying that most breaches occur due to employee error. SC Magazine

Full Story :
http://www.scmagazineus.com/SC-World-Congress-Worker-training-key-to-data-protection/article/152189/

- **SC World Congress: Forensic tips in court**

Computer forensics experts called to testify before a judge and jury must relay the facts of the case but equally important, must convey them in a way a jury can understand.

On the witness stand, a computer forensic expert must also establish himself or herself as a reliable source, Mark Pollitt, visiting professor at the National Center for Forensic Science at the University of Central Florida, said Tuesday at the SC World Congress in a session called "Forensics for Court."

The goal, he said, is to establish personal credibility, relay the facts of the case clearly, ensure the judge and jury comprehend the facts and, finally, to be likable. SC Magazine

Full Story :
http://www.scmagazineus.com/SC-World-Congress-Forensic-tips-in-court/article/152181/

- **New Ad-Aware offers behavioral detection**

Lavasoft has updated its popular malware and spyware detection and removal tool Ad-Aware. Rather than a dramatic redo, version 8.1 builds on the improvements made in the previous version. The new version is faster, has better removal abilities, and introduces a behavioral detection engine.

Ad-Aware 8 Called Genotype, Ad-Aware's heuristic-based behavioral detection engine isn't explicitly called out in the interface. However, I noticed that files that had been flagged falsely as threats in earlier versions were no longer called out as such, and the Quick Scan was able to complete in about three minutes, as opposed to 10 minutes in the previous version. These are empirical observations, of course, but this version's improvements should be easy to see for longtime users of Ad-Aware. Cnet Security

Full Story :
http://download.cnet.com/8301-2007_4-10371489-12.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

- **18554 SMBv2 Infinite Loop Vulnerability (MS09-050/975517) (Remote File Checking)**

A denial of service vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB version 2 (SMBv2) packets. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the Server service. An attacker who successfully exploited this vulnerability could cause the computer to stop responding until restarted.

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

References:

* MS: ms09-050
http://www.microsoft.com/technet/security/bulletin/ms09-050.mspx
* BID: 36595
http://www.securityfocus.com/bid/36595

CVE Reference:

CVE-2009-2526 (cve.mitre.org, nvd.nist.gov)

- **18555 SMBv2 Command Value Vulnerability (MS09-050/975517) (Remote File Checking)**

An unauthenticated remote code execution vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a

computer running the Server service. An attacker who successfully exploited this vulnerability could take complete control of the system.

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

References:

* MS: ms09-050
http://www.microsoft.com/technet/security/bulletin/ms09-050.mspx
* BID: 36594
http://www.securityfocus.com/bid/36594

CVE Reference:

CVE-2009-2532 (cve.mitre.org, nvd.nist.gov)

• 18556 SMBv2 Negotiation Vulnerability (MS09-050/975517) (Remote File Checking)

An unauthenticated remote code execution vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB packet to a computer running the Server service. An attacker who successfully exploited this vulnerability could take complete control of the system.

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

References:

* MS: ms09-050
http://www.microsoft.com/technet/security/bulletin/ms09-050.mspx
* FULLDISC: 20090907 Windows Vista/7 : SMB2.0 NEGOTIATE PROTOCOL REQUEST Remote B.S.O.D.
http://archives.neohapsis.com/archives/fulldisclosure/2009-09/0090.html
* MISC:
http://g-laurent.blogspot.com/2009/09/windows-vista7-smb20-negotiate-protocol.html
* MISC:
http://isc.sans.org/diary.html?storyid=7093
* BID: 36299
http://www.securityfocus.com/bid/36299
* SECUNIA: 36623
http://secunia.com/advisories/36623

CVE Reference:

CVE-2009-3103 (cve.mitre.org, nvd.nist.gov)

• 18557 Internet Explorer Data Stream Header Corruption Vulnerability (MS09-054/974455) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer processes data stream headers in specific situations. 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. 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.

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

References:

* MS: ms09-054
http://www.microsoft.com/technet/security/bulletin/ms09-054.mspx
* BID: 36622
http://www.securityfocus.com/bid/36622

CVE Reference:

CVE-2009-1547 (cve.mitre.org, nvd.nist.gov)

• 18558 Internet Explorer HTML Component Handling Vulnerability (MS09-054/974455) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer handles argument validation of a variable in specific situations. 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. 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.

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

References:

* MS: ms09-054
http://www.microsoft.com/technet/security/bulletin/ms09-054.mspx
* BID: 36621
http://www.securityfocus.com/bid/36621

CVE Reference:

CVE-2009-2529 (cve.mitre.org, nvd.nist.gov)

• 18559 Internet Explorer Uninitialized Memory Corruption Vulnerability (CVE-2009-2530) (MS09-054/974455) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer accesses an object that has not been correctly initialized or 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. 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.

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

References:

* MS: ms09-054
http://www.microsoft.com/technet/security/bulletin/ms09-054.mspx
* BID: 36620
http://www.securityfocus.com/bid/36620

CVE Reference:

CVE-2009-2530 (cve.mitre.org, nvd.nist.gov)

• 18560 Internet Explorer Uninitialized Memory Corruption Vulnerability (CVE-2009-2531) (MS09-054/974455) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer accesses an object that has not been correctly initialized or 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. 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.

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

References:

* MS: ms09-054
http://www.microsoft.com/technet/security/bulletin/ms09-054.mspx
* BID: 36616
http://www.securityfocus.com/bid/36616

CVE Reference:

CVE-2009-2531 (cve.mitre.org, nvd.nist.gov)

• 18561 Windows Kernel Integer Underflow Vulnerability (MS09-058/971486) (Remote File Checking)

An elevation of privilege vulnerability exists in the Windows kernel due to the incorrect truncation of a 64-bit value to a 32-bit value. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

* MS: ms09-058
http://www.microsoft.com/technet/security/bulletin/ms09-058.mspx

* BID: 36623
http://www.securityfocus.com/bid/36623

CVE Reference:

CVE-2009-2515 (cve.mitre.org, nvd.nist.gov)

- **18562 Windows Kernel NULL Pointer Dereference Vulnerability (MS09-058/971486) (Remote File Checking)**

An elevation of privilege vulnerability exists in the Windows kernel due to the insufficient validation of certain data passed from user mode. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

* MS: ms09-058
http://www.microsoft.com/technet/security/bulletin/ms09-058.mspx
* BID: 36624
http://www.securityfocus.com/bid/36624

CVE Reference:

CVE-2009-2516 (cve.mitre.org, nvd.nist.gov)

- **18563 Windows Kernel Exception Handler Vulnerability (MS09-058/971486) (Remote File Checking)**

A denial of service vulnerability exists in the Windows kernel because of the way the kernel handles certain exceptions. An attacker could exploit the vulnerability by running a specially crafted application causing the system to restart.

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

References:

* MS: ms09-058
http://www.microsoft.com/technet/security/bulletin/ms09-058.mspx
* BID: 36625
http://www.securityfocus.com/bid/36625

CVE Reference:

CVE-2009-2517 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2009-2532 Microsoft CVSS 2.0 Score = 10.0**

Microsoft Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold and SP2, and Windows 7 RC do not properly process the command value in an SMB Multi-Protocol Negotiate Request packet, which allows remote attackers to execute arbitrary code via a crafted SMBv2 packet to the Server service, aka "SMBv2 Command Value Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-050.mspx

CVE Reference: CVE-2009-2532

- **CVE-2009-0090 Microsoft CVSS 2.0 Score = 9.3**

Microsoft .NET Framework 1.0 SP3, 1.1 SP1, and 2.0 SP1 does not properly validate .NET verifiable code, which allows remote attackers to obtain unintended access to stack memory, and execute arbitrary code, via (1) a crafted XAML browser application (XBAP), (2) a crafted ASP.NET application, or (3) a crafted .NET Framework application, aka "Microsoft .NET Framework Pointer Verification Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-061.mspx

CVE Reference: CVE-2009-0090

- **CVE-2009-0091 Microsoft CVSS 2.0 Score = 9.3**

Microsoft .NET Framework 2.0, 2.0 SP1, and 3.5 does not properly enforce a certain type-equality constraint in .NET verifiable code, which allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP), (2) a crafted ASP.NET application, or (3) a crafted .NET Framework application, aka "Microsoft .NET Framework Type Verification Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-061.mspx

CVE Reference: CVE-2009-0091

- **CVE-2009-0555 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Windows Media Runtime, as used in DirectShow WMA Voice Codec, Windows Media Audio Voice Decoder, and Audio Compression Manager (ACM), does not properly process Advanced Systems Format (ASF) files, which allows remote attackers to execute arbitrary code via a crafted audio file that uses the Windows Media Speech codec, aka "Windows Media Runtime Voice Sample Rate Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-051.mspx

CVE Reference: CVE-2009-0555

- **CVE-2009-1547 Microsoft CVSS 2.0 Score = 9.3**

Unspecified vulnerability in Microsoft Internet Explorer 5.01 SP4, 6, 6 SP1, and 7 allows remote attackers to execute arbitrary code via a crafted data stream header that triggers memory corruption, aka "Data Stream Header Corruption Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-054.mspx

CVE Reference: CVE-2009-1547

- **CVE-2009-2497 Microsoft CVSS 2.0 Score = 9.3**

The Common Language Runtime (CLR) in Microsoft .NET Framework 2.0, 2.0 SP1, 2.0 SP2, 3.5, and 3.5 SP1, and Silverlight 2, does not properly handle interfaces, which allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP), (2) a crafted Silverlight application, (3) a crafted ASP.NET application, or (4) a crafted .NET Framework application, aka "Microsoft Silverlight and Microsoft .NET Framework CLR Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-061.mspx

CVE Reference: CVE-2009-2497

- **CVE-2009-2500 Microsoft CVSS 2.0 Score = 9.3**

Integer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a crafted WMF image file, aka "GDI+ WMF Integer Overflow Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-062.mspx

CVE Reference: CVE-2009-2500

- **CVE-2009-2501 Microsoft CVSS 2.0 Score = 9.3**

Heap-based buffer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a crafted PNG image file, aka "GDI+ PNG Heap Overflow Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-062.mspx

CVE Reference: CVE-2009-2501

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