ScoutNews
The weekly Security update from the makers of SecureScout
October 10, 2008

2008 Issue #41

Table of Contents

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

DNS roots to become more secure. More on click-jacking - what it actually is. Massive data loss in UK. The economic crisis helps malware spread.

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

- **U.S. proposes digital signing of DNS root zone file**

October 10, 2008 (IDG News Service) The U.S. government is seeking input on a way to make the Internet's addressing system less susceptible to tampering by hackers.

The U.S. Department of Commerce is asking for comments through Nov. 24 on how DNSSEC could best be deployed.

But several security problems within the DNS make it possible for hackers to supply a different IP address for a Web site. It means users think they are viewing www.computerworld.com but are on a phishing site.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9116900&source=rss_topic1

- **Researchers reveal \'clickjacking\' attack info**

October 8, 2008 (Computerworld) The security researchers who two weeks ago warned of new "clickjacking" vulnerabilities in browsers, Web sites and popular plug-ins, revealed a dozen variants of the bug yesterday.

On Tuesday, Hansen disclosed more information about "clickjacking," the new class of vulnerabilities that he and

fellow researcher Jeremiah Grossman, the chief technology officer at WhiteHat Security Inc., first mentioned during a semi-closed presentation at a New York security conference on Sept. 24. Hansen and Grossman had originally intended to present the bulk of their findings then, but agreed to withhold most of the information at the request of Adobe, which said it would quickly patch its software against clickjacking attack.

With the cat out of the bag, Adobe gave Hansen and Grossman the go-ahead to get specific about their findings. Hansen then posted a list of 12 different clickjacking scenarios on his blog.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9116638&source=rss_topic1

- **Over half of U.K. firms have lost data**

October 10, 2008 (Computerworld UK) An astonishing 55% of British companies have lost data, according to a new report of 785 IT professionals in the U.K.

Around two-thirds of respondents said negligence, including that of outsourcers, was responsible for data breaches, compared with only 10% who said hackers were a major cause. A third said insiders were a threat.

Only 3% were tracking changes made to data, such as when account details are updated, even though 91% said this was an important part of tackling the problem.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9116919&source=rss_topic1

- **Economic woes fueling spam malware barrage**

Two monthly threat reports released this week show a sharp increase in emails containing malware.

The rise appears to be bolstered by the current fiscal crisis, which is providing cybercriminals with fodder for their scam campaigns, according to MX Logic.

The security firm said 5.14 percent of all emails in September contained malware, more than seven times the average and largest jump since February 2007, when the Storm Worm first appeared.

SC Magazine

Full Story :
http://www.scmagazineus.com/Economic-woes-fueling-spam-malware-barrage/article/119152/

New Vulnerabilities found this Week

- **CVE-2008-4493 Microsoft CVSS 2.0 Score = 6.8**

Microsoft PicturePusher ActiveX control (PipPPush.DLL 7.00.0709), as used in Microsoft Digital Image 2006 Starter Edition, allows remote attackers to force the upload of arbitrary files by using the AddString and Post methods and a modified PostURL to construct an HTTP POST request. NOTE: this issue might only be exploitable in limited environments or non-default browser settings.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/45735

SECTRACK: http://www.securitytracker.com/id?1021018

BID: http://www.securityfocus.com/bid/31632

MILW0RM: http://www.milw0rm.com/exploits/6699

CVE Reference: CVE-2008-4493

- **CVE-2008-4510 Microsoft CVSS 2.0 Score = 4.9**

Microsoft Windows Vista Home and Ultimate Edition SP1 and earlier allows local users to cause a denial of service (page fault and system crash) via multiple attempts to access a virtual address in a PAGE_NOACCESS memory

page.

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

References:

BID: http://www.securityfocus.com/bid/31570

MILW0RM: http://www.milw0rm.com/exploits/6671

SECUNIA: http://secunia.com/advisories/32115

CVE Reference: CVE-2008-4510

- **CVE-2008-4482 Apache CVSS 2.0 Score = 7.8**

The XML parser in Xerces-C++ before 3.0.0 allows context-dependent attackers to cause a denial of service (stack consumption and crash) via an XML schema definition with a large maxOccurs value, which triggers excessive memory consumption during validation of an XML file.

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

References:

BID: http://www.securityfocus.com/bid/31533

CONFIRM: http://xerces.apache.org/xerces-c/releases.html

SECUNIA: http://secunia.com/advisories/32108

MISC: http://issues.apache.org/jira/browse/XERCESC-1051

CVE Reference: CVE-2008-4482

- **CVE-2008-3543 HP CVSS 2.0 Score = 7.8**

Unspecified vulnerability in NFS / ONCplus B.11.31_04 and earlier on HP-UX B.11.31 allows remote attackers to cause a denial of service via unknown attack vectors.

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

References:

HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01570585

XF: http://xforce.iss.net/xforce/xfdb/45695

SECTRACK: http://www.securitytracker.com/id?1020993

BID: http://www.securityfocus.com/bid/31607

FRSIRT: http://www.frsirt.com/english/advisories/2008/2748

SECUNIA: http://secunia.com/advisories/32161

HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01570585

CVE Reference: CVE-2008-3543

- **CVE-2008-4505 IBM CVSS 2.0 Score = 7.8**

Unspecified vulnerability in IBM Lotus Quickr 8.1 before Fix pack 1 (8.1.0.1) might allow attackers to cause a denial of service (system crash) via a "nonstandard URL argument" to the OpenDocument command. NOTE: due to lack of details from the vendor, it is not clear whether this is a vulnerability.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/45692

BID: http://www.securityfocus.com/bid/31608

FRSIRT: http://www.frsirt.com/english/advisories/2008/2753

CONFIRM: http://www-01.ibm.com/support/docview.wss?uid=swg27013341

SECUNIA: http://secunia.com/advisories/32098

CVE Reference: CVE-2008-4505

- **CVE-2008-4506 IBM CVSS 2.0 Score = 7.5**

Unspecified vulnerability in IBM Lotus Quickr 8.1 before Fix pack 1 (8.1.0.1) allows a place manager to "demote or delete a place superuser group" via unknown vectors.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/45694

BID: http://www.securityfocus.com/bid/31608

FRSIRT: http://www.frsirt.com/english/advisories/2008/2753

CONFIRM: http://www-01.ibm.com/support/docview.wss?uid=swg27013341

SECUNIA: http://secunia.com/advisories/32098

CVE Reference: CVE-2008-4506

- **CVE-2008-4507 IBM CVSS 2.0 Score = 7.5**

Unspecified vulnerability in IBM Lotus Quickr 8.1 before Fix pack 1 (8.1.0.1) allows editors to delete pages that were created by a different author via unknown vectors.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/45693

BID: http://www.securityfocus.com/bid/31608

FRSIRT: http://www.frsirt.com/english/advisories/2008/2753

CONFIRM: http://www-01.ibm.com/support/docview.wss?uid=swg27013341

SECUNIA: http://secunia.com/advisories/32098

CVE Reference: CVE-2008-4507

- **CVE-2008-3814 Cisco CVSS 2.0 Score = 9.3**

Unspecified vulnerability in Cisco Unity 4.x before 4.2(1)ES161, 5.x before 5.0(1)ES53, and 7.x before 7.0(2)ES8, when using anonymous authentication (aka native Unity authentication), allows remote attackers to bypass authentication and read or modify system configuration parameters by going to a specific link more than once.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080a0d85f.shtml

MISC: http://www.voipshield.com/research-details.php?id=126

BID: http://www.securityfocus.com/bid/31642

FRSIRT: http://www.frsirt.com/english/advisories/2008/2771

CISCO: http://www.cisco.com/en/US/products/products_security_response09186a0080a0d861.html

SECUNIA: http://secunia.com/advisories/32187

CVE Reference: CVE-2008-3814

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