ScoutNews
The weekly Security update from the makers of SecureScout
December 19, 2008

2008 Issue #51

Table of Contents

Product Focus

Spida Digispid Worm Scanner - The S4 Spida Digispid Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are prone any of the Microsoft Java Virtual Machine Vulnerabilities (MS02-069).

Download Here:
http://www.netvigilance.com/productdownloads?productname=spidadigispidwormscanner

This Week in Review

No recession expected for cyber crime in 2009. Clarification needed on vpn and wireless security. Some protection possible when using social networks. Collaboration applications are cool but not safe.

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

- **2009 security predictions: Deja vu all over again**

December 17, 2008 (Computerworld) The security industry is fueled largely by FUD (fear, uncertainty and doubt.) So it's not unusual for most forecasts in the industry to be full of grim prognostications of imminent chaos and calamities.

Most of the security vendors' forecasts predict dramatic spikes in volumes of spam, phishing, botnet activity and malware targeted at companies. The reports also highlight sharp increases in attacks directed against Web and mobile applications. But the concerns largely deal with issues that security managers are already familiar with, and there are few, if any, really nasty new threats in store around the corner, according to the forecasts.

Together, the forecasts paint a picture of a threat environment that, while not pretty, looks largely like the one this past year — except that it will have more of everything. Among the forecasts are the following:

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9123780&source=rss_topic1

- **Wireless VPNs: Protecting the wireless wanderer**

December 16, 2008 (CSO) Picture this: road warriors wirelessly connecting to the corporate network from hot spots at airports or coffee outlets. Just a few years ago, nightmare stories were common of even casual bystanders being able to eavesdrop on corporate communications made in such circumstances. As a result, there's a widespread acceptance that virtual private networks (VPN) are pretty much de rigueur for wireless use on the road.

"People tend to fixate on the word private in 'virtual private network,' '" says Jeremy Cioara, an author of five books for Cisco Press and a security instructor for training provider CBT Nuggets in Eugene, Ore. "They're sitting in Starbucks working at their laptop, and they think that because they're using a VPN, it's safe. It isn't."

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9123468&source=rss_topic1

- **3 ways to protect yourself from social networking malware**

December 17, 2008 (CIO) As social networking tools change the way we communicate, spammers have begun turning their attention to services such as Facebook and MySpace, tricking users into installing viruses, launching fraudulent Web sites and deploying malware throughout their computers and networks, according to a a new report by MessageLabs.

Luckily, if you're wading in the social networking pool, you can revisit some core security principles in order to protect yourself from spammers and other characters on Facebook who can ruin your computer or identity, Sergeant says.

In a lawsuit, which Facebook won for an amount just shy of $900 million, the social network alleged that the spammer sent out four million spam messages from accounts in which he had obtained the passwords.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9123778&source=rss_topic1

- **Survey: Collaboration applications inadequately secured**

Updated Thursday, Dec. 18, 2008 at 3:32 p.m. EST

There is a lapse around the security of collaboration applications used in enterprises, concludes a survey by access management vendor Rohati.

To improve communication and responsiveness among employees, enterprises utilize collaboration applications such as web-based intranet portals, common internet file systems (CIFS) and Microsoft SharePoint.

SC Magazine

Full Story :
http://www.scmagazineus.com/Survey-Collaboration-applications-inadequately-secured/article/123081/

New Vulnerabilities Tested in SecureScout

- **18226 GDI Integer Overflow Vulnerability (MS08-071/956802) (Remote File Checking)**

A remote code execution vulnerability exists in the way that GDI handles integer calculations. The vulnerability could allow remote code execution if a user opens a specially crafted WMF image file. 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.

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

References:

* MS: MS08-071
http://www.microsoft.com/technet/security/Bulletin/MS08-071.mspx
* BID: 32634
http://www.securityfocus.com/bid/32634
* FRSIRT: Microsoft Windows GDI Two Remote Code Execution Vulnerabilities (MS08-071)
http://www.vupen.com/english/advisories/2008/3383

* SECUNIA: 33020
http://secunia.com/Advisories/33020/

CVE Reference:

CVE-2008-2249 (cve.mitre.org, nvd.nist.gov)

• 18227 GDI Heap Overflow Vulnerability (MS08-071/956802) (Remote File Checking)

A remote code execution vulnerability exists in the way that GDI handles file size parameters in WMF files. The vulnerability could allow remote code execution if a third-party application uses a specific Microsoft API to copy a specially crafted WMF image file. 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.

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

References:

* MS: MS08-071
http://www.microsoft.com/technet/security/Bulletin/MS08-071.mspx
* BID: 32637
http://www.securityfocus.com/bid/32637
* FRSIRT: Microsoft Windows GDI Two Remote Code Execution Vulnerabilities (MS08-071)
http://www.vupen.com/english/advisories/2008/3383
* SECUNIA: 33020
http://secunia.com/Advisories/33020/

CVE Reference:

CVE-2008-3465 (cve.mitre.org, nvd.nist.gov)

• 18228 Windows Saved Search Vulnerability (MS08-075/959349) (Remote File Checking)

A remote code execution vulnerability exists when saving a specially crafted search file within Windows Explorer. This operation causes Windows Explorer to exit and restart in an exploitable manner.

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

References:

* MS: MS08-075
http://www.microsoft.com/technet/security/Bulletin/MS08-075.mspx
* FRSIRT: Microsoft Windows Search Code Execution Vulnerabilities (MS08-075)
http://www.vupen.com/english/advisories/2008/3387
* SECUNIA: 33053
http://secunia.com/advisories/33053/
* BID: 32651
http://www.securityfocus.com/bid/32651

CVE Reference:

CVE-2008-4268 (cve.mitre.org, nvd.nist.gov)

• 18229 Windows Search Parsing Vulnerability (MS08-075/959349) (Remote File Checking)

A remote code execution vulnerability exists in Windows Explorer that allows an attacker to construct a malicious web page that includes a call to the search-ms protocol handler. The protocol handler in turn passes untrusted data to Windows Explorer.

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

References:

* MS: MS08-075
http://www.microsoft.com/technet/security/Bulletin/MS08-075.mspx
* BID: 32652
http://www.securityfocus.com/bid/32652
* FRSIRT: Microsoft Windows Search Code Execution Vulnerabilities (MS08-075)
http://www.vupen.com/english/advisories/2008/3387
* SECUNIA: 33053
http://secunia.com/advisories/33053/

CVE Reference:

CVE-2008-4269 (cve.mitre.org, nvd.nist.gov)

• 18230 Internet Explorer Parameter Validation Memory Corruption Vulnerability (MS08-073/958215) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer handles certain navigation methods. 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: MS08-073
http://www.microsoft.com/technet/security/Bulletin/MS08-073.mspx
* FRSIRT: Microsoft Internet Explorer Code Execution Vulnerabilities (MS08-073)
http://www.vupen.com/english/advisories/2008/3385
* SECTRACK: 1021371
http://securitytracker.com/alerts/2008/Dec/1021371.html
* SECUNIA: 33035
http://secunia.com/advisories/33035/
* BID: 32596
http://www.securityfocus.com/bid/32596

CVE Reference:

CVE-2008-4258 (cve.mitre.org, nvd.nist.gov)

• 18231 Internet Explorer HTML Objects Memory Corruption Vulnerability (MS08-073/958215) (Remote File Checking)

A remote code execution vulnerability exists in Internet Explorer due to attempts to access uninitialized memory in certain 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.

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

References:

* MS: MS08-073
http://www.microsoft.com/technet/security/Bulletin/MS08-073.mspx
* FRSIRT: Microsoft Internet Explorer Code Execution Vulnerabilities (MS08-073)
http://www.vupen.com/english/advisories/2008/3385
* SECTRACK: 1021371
http://securitytracker.com/alerts/2008/Dec/1021371.html
* SECUNIA: 33035
http://secunia.com/advisories/33035/
* BID: 32586
http://www.securityfocus.com/bid/32586

CVE Reference:

CVE-2008-4259 (cve.mitre.org, nvd.nist.gov)

• 18232 Internet Explorer Uninitialized Memory Corruption Vulnerability (MS08-073/958215) (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: MS08-073
http://www.microsoft.com/technet/security/Bulletin/MS08-073.mspx
* FRSIRT: Microsoft Internet Explorer Code Execution Vulnerabilities (MS08-073)
http://www.vupen.com/english/advisories/2008/3385
* SECTRACK: 1021371
http://securitytracker.com/alerts/2008/Dec/1021371.html
* SECUNIA: 33035
http://secunia.com/advisories/33035/

* BID: 32593
http://www.securityfocus.com/bid/32593

CVE Reference:

CVE-2008-4260 (cve.mitre.org, nvd.nist.gov)

• 18233 Internet Explorer HTML Rendering Memory Corruption Vulnerability (MS08-073/958215) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer embeds objects into a Web page. 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: MS08-073
http://www.microsoft.com/technet/security/Bulletin/MS08-073.mspx
* BID: 32595
http://www.securityfocus.com/bid/32595
* FRSIRT: Microsoft Internet Explorer Code Execution Vulnerabilities (MS08-073)
http://www.vupen.com/english/advisories/2008/3385
* SECTRACK: 1021371
http://securitytracker.com/alerts/2008/Dec/1021371.html
* SECUNIA: 33035
http://secunia.com/advisories/33035/

CVE Reference:

CVE-2008-4261 (cve.mitre.org, nvd.nist.gov)

• 18234 Windows Media Components SPN Vulnerability (MS08-076/959807) (Remote File Checking)

A credential reflection vulnerability exists in the Windows Media components that could allow an attacker to execute code with the same rights as the local user or with Windows Media Services distribution credentials. The vulnerability exists due to weaknesses in Service Principal Name (SPN) implementations within Windows Media components.

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

References:

* FRSIRT: Microsoft Windows Media Products Code Execution Vulnerabilities (MS08-076)
http://www.vupen.com/english/advisories/2008/3388
* SECUNIA: 33058
http://secunia.com/advisories/33058/
* MS: MS08-076
http://www.microsoft.com/technet/security/Bulletin/MS08-076.mspx
* BID: 32653
http://www.securityfocus.com/bid/32653

CVE Reference:

CVE-2008-3009 (cve.mitre.org, nvd.nist.gov)

• 18235 Windows Media Components ISATAP Vulnerability (MS08-076/959807) (Remote File Checking)

An information disclosure vulnerability exists in supported versions of Windows Media components that could result in the disclosure of NTLM credentials. Any Windows Media component that accesses a URL that uses an ISATAP address could leak the userâ's NTLM credentials to the server that hosts the URL. This could allow an attacker who is external to the intranet zone to gather NTLM credentials for an enterprise environment.

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

References:

* MS: MS08-076
http://www.microsoft.com/technet/security/Bulletin/MS08-076.mspx
* FRSIRT: Microsoft Windows Media Products Code Execution Vulnerabilities (MS08-076)
http://www.vupen.com/english/advisories/2008/3388
* BID: 32654
http://www.securityfocus.com/bid/32654

* SECUNIA: 33058
http://secunia.com/advisories/33058/

CVE Reference:

CVE-2008-3010 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-5624 PHP CVSS 2.0 Score = 7.5

PHP 5 before 5.2.7 does not properly initialize the page_uid and page_gid global variables for use by the SAPI php_getuid function, which allows context-dependent attackers to bypass safe_mode restrictions via variable settings that are intended to be restricted to root, as demonstrated by a setting of /etc for the error_log variable.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/47318

BID: http://www.securityfocus.com/bid/32688

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/498985/100/0/threaded

CONFIRM: http://www.php.net/ChangeLog-5.php#5.2.7

SREASONRES: http://securityreason.com/achievement_securityalert/59

CVE Reference: CVE-2008-5624

• CVE-2008-5625 PHP CVSS 2.0 Score = 7.5

PHP 5 before 5.2.7 does not enforce the error_log safe_mode restrictions when safe_mode is enabled through a php_admin_flag setting in httpd.conf, which allows context-dependent attackers to write to arbitrary files by placing a "php_value error_log" entry in a .htaccess file.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/47314

BID: http://www.securityfocus.com/bid/32383

CONFIRM: http://www.php.net/ChangeLog-5.php#5.2.7

SREASONRES: http://securityreason.com/achievement_securityalert/57

CVE Reference: CVE-2008-5625

• CVE-2008-5658 PHP CVSS 2.0 Score = 7.5

Directory traversal vulnerability in the ZipArchive::extractTo function in PHP 5.2.6 and earlier allows context-dependent attackers to write arbitrary files via a ZIP file with a file whose name contains .. (dot dot) sequences.

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

References:

MISC: http://www.sektioneins.de/advisories/SE-2008-06.txt

CONFIRM: http://www.php.net/ChangeLog-5.php#5.2.7

MLIST: http://www.openwall.com/lists/oss-security/2008/12/04/3

CVE Reference: CVE-2008-5658

• CVE-2008-4220 Apple CVSS 2.0 Score = 10.0

Integer overflow in the inet_net_pton API in Libsystem in Apple Mac OS X before 10.5.6 allows context-dependent attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors. NOTE: this may be related to the WLB-2008080064 advisory published by SecurityReason on 20080822; however, as of

20081216, there are insufficient details to be sure.

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

References:

CERT: http://www.us-cert.gov/cas/techalerts/TA08-350A.html

BID: http://www.securityfocus.com/bid/32839

CONFIRM: http://support.apple.com/kb/HT3338

APPLE: http://lists.apple.com/archives/security-announce//2008//Dec/msg00000.html

CVE Reference: CVE-2008-4220

- **CVE-2008-4221 Apple CVSS 2.0 Score = 10.0**

The strptime API in Libsystem in Apple Mac OS X before 10.5.6 allows context-dependent attackers to cause a denial of service (memory corruption and application crash) or execute arbitrary code via a crafted date string, related to improper memory allocation.

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

References:

CERT: http://www.us-cert.gov/cas/techalerts/TA08-350A.html

BID: http://www.securityfocus.com/bid/32839

CONFIRM: http://support.apple.com/kb/HT3338

APPLE: http://lists.apple.com/archives/security-announce//2008//Dec/msg00000.html

CVE Reference: CVE-2008-4221

- **CVE-2008-4223 Apple CVSS 2.0 Score = 10.0**

Podcast Producer in Apple Mac OS X 10.5 before 10.5.6 allows remote attackers to bypass authentication and gain administrative access via unspecified vectors.

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

References:

CERT: http://www.us-cert.gov/cas/techalerts/TA08-350A.html

BID: http://www.securityfocus.com/bid/32839

CONFIRM: http://support.apple.com/kb/HT3338

APPLE: http://lists.apple.com/archives/security-announce//2008//Dec/msg00000.html

CVE Reference: CVE-2008-4223

- **CVE-2008-4237 Apple CVSS 2.0 Score = 10.0**

Managed Client in Apple Mac OS X before 10.5.6 sometimes misidentifies a system when installing per-host configuration settings, which allows context-dependent attackers to have an unspecified impact by leveraging unintended settings, as demonstrated by the screen saver lock setting.

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

References:

CERT: http://www.us-cert.gov/cas/techalerts/TA08-350A.html

BID: http://www.securityfocus.com/bid/32839

CONFIRM: http://support.apple.com/kb/HT3338

APPLE: http://lists.apple.com/archives/security-announce//2008//Dec/msg00000.html

CVE Reference: CVE-2008-4237

- **CVE-2008-5500 Mozilla CVSS 2.0 Score = 10.0**

The layout engine in Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 allows remote attackers to cause a denial of service (crash) and possibly trigger memory corruption via vectors related to (1) a reahable assertion or (2) an integer overflow.Per http://www.mozilla.org/security/announce/2008/mfsa2008-60.html Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code. Thunderbird shares the browser engine with Firefox and could be vulnerable if JavaScript were to be enabled in mail. This is not the default setting and we strongly discourage users from running JavaScript in mail. Without further investigation we cannot rule out the possibility that for some of these an attacker might be able to prepare memory for exploitation through some means other than JavaScript such as large images.

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

References:

MISC: https://bugzilla.mozilla.org/show_bug.cgi?id=464998

MISC: https://bugzilla.mozilla.org/show_bug.cgi?id=460803

CONFIRM: http://www.mozilla.org/security/announce/2008/mfsa2008-60.html

CVE Reference: CVE-2008-5500

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