

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

[Sasser Worm Scanner](#) - The S4 Sasser Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Microsoft SSL Vulnerability (MS04-011) that used by the Sasser Worm to infect machines.

Download Here:

<http://www.netvigilance.com/productdownloads?productname=sasserwormscanner>

This Week in Review

Commission recommend cybersecurity handed over to the White House. Cloud computing the next security issue. Organizations team up to look at dns security. Security difficult in social networks.

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: Commission on cybersecurity releases recommendations

Cybersecurity control should be taken away from the U.S. Department of Homeland Security placed under the White House's purview, a panel of government and industry leaders are urging President-elect Barack Obama.

"This new office can help begin the work of building an 'information age' government, based on the new, more collaborative organizational models found in business," the report said.

Following a number of high-profile government computer breaches, the commission was established at the end of 2007 by the Center for Strategic and International Studies (CSIS) and co-chaired by U.S. Reps. Jim Langevin, D-R.I. and Michael McCaul, R-Texas.

SC Magazine

Full Story :

<http://www.scmagazineus.com/SC-World-Congress-Commission-on-cybersecurity-releases-recommendations/article>

• SC World Congress: Cloud computing presents next challenge

If you thought deperimeterization was a daunting concept, you haven't seen anything yet â€” try securing cloud computing, concluded board members of Jericho Forum Monday.

Speaking at the Jericho Forum's "Breaking Down the Barriers to Secure Collaboration" panel discussion, held in conjunction with this week's inaugural SC World Congress, Paul Simmonds and other panelists discussed the challenges that deperimeterization and cloud computing pose to global enterprises.

Cloud computing will enable businesses to function more efficiently and collaborate with other organizations, but they must recognize the security ramifications, such as safeguarding data and managing identities, the panel said.

SC Magazine

Full Story :

<http://www.scmagazineus.com/SC-World-Congress-Cloud-computing-presents-next-challenge/article/122288/>

• VeriSign, NeuStar and others team on DNS security

December 9, 2008 (Network World) Momentum continues to build for rapid deployment of DNS encryption mechanisms.

DNSSEC prevents hackers from hijacking Web traffic and redirecting it to bogus sites. The Internet standard prevents spoofing attacks by allowing Web sites to verify their domain names and corresponding IP addresses using digital signatures and public-key encryption.

DNSSEC is viewed as the best way to bolster the DNS against vulnerabilities such as the Kaminsky bug discovered this summer. It's because of threats such as these that the U.S. government is rolling out DNSSEC across its .gov and .mil domains.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9123026&source=rss_topic1

• Cybercrime '09: Too late to save Facebook?

December 9, 2008 (CSO) A warning to those who love such social media sites as Facebook: The bad guys are coming for you.

The findings on Flash and PDF are presented in a report released on Tuesday from security products firm Finjan Inc. The research finds that cybercriminals are increasingly using PDF and Flash files as vehicles for distributing their malicious code and for infecting end-user PCs.

The report states that large advertising networks serving Flash-based banner ads did not prevent their ads from interacting with the hosting Web page. The lack of configuration by ad networks to prevent this interaction, between the served Flash-based ad's Action Script and the DOM, has become a new vector for cybercriminals to serve their malicious code undetected.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9123022&source=rss_topic1

New Vulnerabilities Tested in SecureScout

• 18238 Excel File Format Parsing Vulnerability (CVE-2008-4264) (MS08-074/959070) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Office Excel as a result of pointer corruption when loading Excel formulas. The vulnerability could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed formula. 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: MS08-074

<http://www.microsoft.com/technet/security/Bulletin/MS08-074.msp>

CVE Reference:

CVE-2008-4264 (cve.mitre.org, nvd.nist.gov)

• **18239 Excel Global Array Memory Corruption Vulnerability (MS08-074/959070) (Remote File Checking)**

A remote code execution vulnerability exists in Microsoft Office Excel as a result of stack corruption when loading Excel records. The vulnerability could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed object. 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: MS08-074

<http://www.microsoft.com/technet/security/Bulletin/MS08-074.msp>

CVE Reference:

CVE-2008-4266 (cve.mitre.org, nvd.nist.gov)

• **18240 Word Memory Corruption Vulnerability (CVE-2008-4024) (MS08-072/957173) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Word handles specially crafted Word files. The vulnerability could allow remote code execution if a user opens a specially crafted Word file with a malformed record. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS08-072

<http://www.microsoft.com/technet/security/Bulletin/MS08-072.msp>

CVE Reference:

CVE-2008-4024 (cve.mitre.org, nvd.nist.gov)

• **18241 Word RTF Object Parsing Vulnerability (CVE-2008-4025) (MS08-072/957173) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office handles specially crafted Rich Text Format (RTF) files. The vulnerability could allow remote code execution if a user opens a specially crafted RTF file in Word or reads a specially crafted e-mail sent in the RTF format. An attacker who successfully exploited this vulnerability could take control of an affected system in the context of the currently logged-on user. 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: MS08-072

<http://www.microsoft.com/technet/security/Bulletin/MS08-072.msp>

CVE Reference:

CVE-2008-4025 (cve.mitre.org, nvd.nist.gov)

• **18242 Word Memory Corruption Vulnerability (CVE-2008-4026) (MS08-072/957173) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Word handles specially crafted Word files. The vulnerability could allow remote code execution if a user opens a specially crafted Word file with a malformed value. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS08-072

<http://www.microsoft.com/technet/security/Bulletin/MS08-072.mspx>

CVE Reference:

CVE-2008-4026 (cve.mitre.org, nvd.nist.gov)

• **18243 Word RTF Object Parsing Vulnerability (CVE-2008-4027) (MS08-072/957173) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office handles specially crafted Rich Text Format (RTF) files. The vulnerability could allow remote code execution if a user opens a specially crafted RTF file with malformed control words in Word, or views or previews a specially crafted RTF file with malformed control words in rich text e-mail. An attacker who successfully exploited this vulnerability could take control of an affected system in the context of the currently logged-on user. 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: MS08-072

<http://www.microsoft.com/technet/security/Bulletin/MS08-072.mspx>

CVE Reference:

CVE-2008-4027 (cve.mitre.org, nvd.nist.gov)

• **18244 Word RTF Object Parsing Vulnerability (CVE-2008-4030) (MS08-072/957173) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office handles specially crafted Rich Text Format (RTF) files. The vulnerability could allow remote code execution if a user opens a specially crafted RTF file in Word or reads or previews a specially crafted e-mail sent in the RTF format. An attacker who successfully exploited this vulnerability could take control of an affected system in the context of the currently logged-in user. 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: MS08-072

<http://www.microsoft.com/technet/security/Bulletin/MS08-072.mspx>

CVE Reference:

CVE-2008-4030 (cve.mitre.org, nvd.nist.gov)

• **18245 Word RTF Object Parsing Vulnerability (CVE-2008-4028) (MS08-072/957173) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office handles specially crafted Rich Text Format (RTF) files. The vulnerability could allow remote code execution if a user opens a specially crafted RTF file in Word, or reads or previews a specially crafted e-mail sent in the RTF format. An attacker who successfully exploited this vulnerability could take control of an affected system in the context of the currently logged-in user. 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: MS08-072

<http://www.microsoft.com/technet/security/Bulletin/MS08-072.mspx>

CVE Reference:

CVE-2008-4028 (cve.mitre.org, nvd.nist.gov)

• **18246 Word RTF Object Parsing Vulnerability (CVE-2008-4031) (MS08-072/957173) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office handles specially crafted Rich Text Format (RTF) files. The vulnerability could allow remote code execution if a user opens a specially crafted RTF file in Word, or reads or previews a specially crafted e-mail sent in the RTF format. An attacker who successfully exploited this vulnerability could take control of an affected system in the context of the currently logged-on user. 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: MS08-072

<http://www.microsoft.com/technet/security/Bulletin/MS08-072.mspx>

CVE Reference:

CVE-2008-4031 (cve.mitre.org, nvd.nist.gov)

• **18247 Word Memory Corruption Vulnerability (CVE-2008-4837) (MS08-072/957173) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office Word handles specially crafted Word files. The vulnerability could allow remote code execution if a user opens a specially crafted Word file that includes a malformed record value. An attacker who successfully exploited this vulnerability could take control of an affected system in the context of the current logged-on user. 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: MS08-072

<http://www.microsoft.com/technet/security/Bulletin/MS08-072.mspx>

CVE Reference:

CVE-2008-4837 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2008-3009 Microsoft CVSS 2.0 Score = 10.0**

Microsoft Windows Media Player 6.4, Windows Media Format Runtime 7.1 through 11, and Windows Media Services 4.1, 9, and 2008 do not properly use the Service Principal Name (SPN) identifier when validating replies to authentication requests, which allows remote servers to execute arbitrary code via vectors that employ NTLM credential reflection, aka "SPN Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-076.mspx>

CVE Reference: [CVE-2008-3009](http://cve.mitre.org)

• **CVE-2008-3010 Microsoft CVSS 2.0 Score = 10.0**

Microsoft Windows Media Player 6.4, Windows Media Format Runtime 7.1 through 11, and Windows Media Services 4.1 and 9 incorrectly associate ISATAP addresses with the Local Intranet zone, which allows remote servers to capture NTLM credentials, and execute arbitrary code through credential-reflection attacks, by sending an authentication request, aka "ISATAP Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-076.mspx>

CVE Reference: [CVE-2008-3010](http://cve.mitre.org)

• **CVE-2008-2249 Microsoft CVSS 2.0 Score = 9.3**

Integer overflow in GDI in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to execute arbitrary code via a malformed header in a crafted WMF file, which triggers a buffer overflow, aka "GDI Integer Overflow Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-071.mspx>

CVE Reference: [CVE-2008-2249](#)

• **CVE-2008-3465 Microsoft CVSS 2.0 Score = 9.3**

Heap-based buffer overflow in an API in GDI in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows context-dependent attackers to cause a denial of service or execute arbitrary code via a WMF file with a malformed file-size parameter, which would not be properly handled by a third-party application that uses this API for a copy operation, aka "GDI Heap Overflow Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-071.msp>

CVE Reference: [CVE-2008-3465](#)

• **CVE-2008-4024 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office Word 2000 SP3 and 2002 SP3 and Office 2004 for Mac allow remote attackers to execute arbitrary code via a crafted Word document that contains a malformed record, which triggers memory corruption, aka "Word Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-072.msp>

CVE Reference: [CVE-2008-4024](#)

• **CVE-2008-4025 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office Word 2000 SP3, 2002 SP3, 2003 SP3, and 2007 Gold and SP1; Outlook 2007 Gold and SP1; Word Viewer 2003 Gold and SP3; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Gold and SP1; Office 2004 and 2008 for Mac; and Open XML File Format Converter for Mac allow remote attackers to execute arbitrary code via a malformed control word in (1) an RTF file or (2) a rich text e-mail message, which triggers incorrect memory allocation and memory corruption, aka "Word RTF Object Parsing Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-072.msp>

CVE Reference: [CVE-2008-4025](#)

• **CVE-2008-4026 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office Word 2000 SP3, 2002 SP3, 2003 SP3, and 2007 Gold and SP1; Word Viewer 2003 Gold and SP3; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Gold and SP1; Office 2004 and 2008 for Mac; and Open XML File Format Converter for Mac allow remote attackers to execute arbitrary code via a crafted Word document that contains a malformed value, which triggers memory corruption, aka "Word Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-072.msp>

CVE Reference: [CVE-2008-4026](#)

• **CVE-2008-4027 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office Word 2000 SP3, 2002 SP3, 2003 SP3, and 2007 Gold and SP1; Outlook 2007 Gold and SP1; Word Viewer 2003 Gold and SP3; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Gold and SP1; and Office 2004 for Mac allow remote attackers to execute arbitrary code via malformed control words in (1) an RTF file or (2) a rich text e-mail message, which triggers a "memory calculation error" and memory corruption, aka "Word RTF Object Parsing Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-072.msp>

CVE Reference: [CVE-2008-4027](#)

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