

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

[Apache Chunked Vulnerability Scanner](#) - The S4 Apache Chunked Vulnerability 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 Apache Chunked Encoding buffer overflow.

Download Here:

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

This Week in Review

Attacks on large companies more widespread than earlier. US authorities teaming up for better security. Botnets on 5 out of every 1000 PCs. Report on worldwide spam.

Industry-Leading OS Detection Using 13 Dimensions Announced

netVigilance is proud to announce that this week's release of the scanning engine contains a major overhaul of the OS Detection code. With this new version, users of all editions of our software will experience vastly improved OS Detection capabilities after updating the software.

This brings the netVigilance level of OS Detection up to our standard of Beyond Compliance, meaning equal to or better than the leading industry standards. Our OS Detection Algorithm will now detect more Operating Systems with superior accuracy. There are clear benefits for netVigilance software scanning users:

- Problem systems can be easily narrowed down by IP and specific operating system
- Scanning speed is further increased due to operating system-specific selection and elimination of test cases
- Better inventory management because the scanning report's specification of Operating System for each network device can be directly used as a basis for IT inventory reports.

This new algorithm utilizes a new state of the art fingerprinting method using an unprecedented 13 dimensions in OS Detection. We have specifically engineered this to be fully scalable and updatable as new operating systems and new versions of existing operating systems are released.

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

- **Most large companies hit by hack attacks, survey shows**

Network World - Is this year turning out to be even worse for getting hacked than last year?

That's what a survey of 350 IT and network professionals would indicate, with large companies in particular reporting this to be worse than last in terms of suffering at least one network intrusion of their user machines, office network or servers.

The Sixth Annual Enterprise IT Security Survey, released Monday, found that 67% of large companies with 5,000 or more employees reported one successful intrusion or more this year, compared with 41% in 2009. Mid-size companies of 1,000 to 4,999 employees fared better with 59% reporting an intrusion, up slightly from 57% in 2009. Computerworld

Full Story :

http://www.computerworld.com/s/article/9190559/Most_large_companies_hit_by_hack_attacks_survey_shows?source=feedburner&utm_source=feedburner&utm_medium=email&utm_campaign=2010-09-20_top_security_news_stories_this_week

- **DoD, DHS to align cybersecurity capabilities**

The U.S. Department of Defense (DoD) and the Department of Homeland Security (DHS) announced plans Tuesday to streamline their cybersecurity capabilities to better protect the nation's networks.

Late last month, Secretary of Homeland Security Janet Napolitano and Secretary of Defense Robert Gates signed an agreement that formalizes processes for the two agencies to work together to protect U.S. networks and critical infrastructure.

The agreement outlines a framework whereby the agencies will provide cybersecurity support to one another, and was intended to improve collaboration as the two departments carry out their respective cybersecurity missions. SC Magazine

Full Story :

http://www.scmagazineus.com/dod-dhs-to-align-cybersecurity-capabilities/article/180992/?utm_source=feedburner&utm_medium=email&utm_campaign=2010-09-20_top_security_news_stories_this_week

- **Microsoft: Over 2 million U.S. PCs caught in botnets**

More than 2 million PCs in the U.S., or 5.2 out of every 1,000, were recruited into botnets during the second quarter of 2010, according to a Microsoft report released yesterday.

The company's ninth and latest Security Intelligence Report tracked the spread of botnets and malware infections detected and removed throughout the world during the first and second quarters of the year. The sheer number of infected PCs found and cleaned up by Microsoft in the U.S. in the second quarter was the highest in the world. But the percentage of infected PCs was greater elsewhere.

(Credit: Microsoft) Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20019602-83.html?part=rss&subj=news&tag=2547-1_3-0-20

- **Report: United States is world's top spammer**

The United States is now the top source of spam, accounting for almost 19 percent of all junk e-mail sent throughout the world, according to a new report out today from Sophos.

The security firm's "Dirty Dozen" report highlighted the top 12 countries responsible for the world's supply of spam during the third quarter. With the United States generating almost 2.5 times more spam than second-place India, the country now accounts for almost one in five junk messages. The United States' 18.6 percent share of all global spam also showed a significant jump from its 15.2 percent share in the second quarter.

(Credit: Sophos) Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20019611-83.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

- **14606 Adobe Acrobat / Reader font-parsing input validation Vulnerability (CVE-2010-3626) (Remote File Checking)**

Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to execute arbitrary code via a crafted font, a different vulnerability than CVE-2010-2889.

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

References:

- * VUPEN: VUPEN/ADV-2010-2573
<http://www.vupen.com/english/advisories/2010/2573>
- * SECTRACK: 1024511
<http://securitytracker.com/alerts/2010/Oct/1024511.html>
- * BID: 43727
<http://www.securityfocus.com/bid/43727>
- * CONFIRM: apsb10-21
<http://www.adobe.com/support/security/bulletins/apsb10-21.html>

CVE Reference:

CVE-2010-3626 (cve.mitre.org, nvd.nist.gov)

• 18953 AutoComplete Information Disclosure Vulnerability (MS10-071/2360131) (Remote File Checking)

An information disclosure vulnerability exists that potentially allows form data within Internet Explorer to be captured via the AutoComplete feature. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow information disclosure if a user viewed the Web page. An attacker who successfully exploited this vulnerability could capture information previously entered into fields after the AutoComplete feature has been enabled.

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

References:

- * MS: MS10-071
<http://www.microsoft.com/technet/security/bulletin/ms10-071.mspx>
- * BID: 43695
<http://www.securityfocus.com/bid/43695>
- * VUPEN: VUPEN/ADV-2010-2618
<http://www.vupen.com/english/advisories/2010/2618>
- * SECTRACK: 1024546
<http://securitytracker.com/alerts/2010/Oct/1024546.html>

CVE Reference:

CVE-2010-0808 (cve.mitre.org, nvd.nist.gov)

• 18954 HTML Sanitization Vulnerability (CVE-2010-3243) (MS10-071/2360131) (Remote File Checking)

An information disclosure vulnerability exists in the way that the toStaticHTML API sanitizes HTML, that could allow an attacker to perform cross-site scripting attacks and run script in the security context of the logged-on user. An attacker who successfully exploited this vulnerability could execute a cross-site scripting attack on the user, allowing the attacker to execute script in the user's security context against a site that is using the toStaticHTML API.

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

References:

- * MS: MS10-071
<http://www.microsoft.com/technet/security/bulletin/ms10-071.mspx>
- * BID: 43703
<http://www.securityfocus.com/bid/43703>
- * VUPEN: VUPEN/ADV-2010-2618
<http://www.vupen.com/english/advisories/2010/2618>
- * SECTRACK: 1024546
<http://securitytracker.com/alerts/2010/Oct/1024546.html>

CVE Reference:

CVE-2010-3243 (cve.mitre.org, nvd.nist.gov)

• 18955 HTML Sanitization Vulnerability (CVE-2010-3324) (MS10-071/2360131) (Remote File Checking)

An information disclosure vulnerability exists in the way that the toStaticHTML API sanitizes HTML, that could allow an attacker to perform cross-site scripting attacks and run script in the security context of the logged-on user. An attacker

who successfully exploited this vulnerability could execute a cross-site scripting attack on the user, allowing the attacker to execute script in the user's security context against a site that is using the toStaticHTML API.

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

References:

- * MS: MS10-071
<http://www.microsoft.com/technet/security/bulletin/ms10-071.msp>
- * BID: 42467
<http://www.securityfocus.com/bid/42467>
- * VUPEN: VUPEN/ADV-2010-2618
<http://www.vupen.com/english/advisories/2010/2618>
- * SECTRACK: 1024546
<http://securitytracker.com/alerts/2010/Oct/1024546.html>

CVE Reference:

CVE-2010-3324 (cve.mitre.org, nvd.nist.gov)

• 18956 CSS Special Character Information Disclosure Vulnerability (MS10-071/2360131) (Remote File Checking)

An information disclosure vulnerability exists in the way that Internet Explorer processes CSS special characters. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow information disclosure if a user viewed the Web page. An attacker who successfully exploited this vulnerability could view content from another domain or Internet Explorer zone.

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

References:

- * MS: MS10-071
<http://www.microsoft.com/technet/security/bulletin/ms10-071.msp>
- * BID: 42993
<http://www.securityfocus.com/bid/42993>
- * VUPEN: VUPEN/ADV-2010-2618
<http://www.vupen.com/english/advisories/2010/2618>
- * SECTRACK: 1024546
<http://securitytracker.com/alerts/2010/Oct/1024546.html>

CVE Reference:

CVE-2010-3325 (cve.mitre.org, nvd.nist.gov)

• 18957 Uninitialized Memory Corruption Vulnerability (CVE-2010-3326) (MS10-071/2360131) (Remote File Checking)

A remote code execution vulnerability exists in the way that 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: MS10-071
<http://www.microsoft.com/technet/security/bulletin/ms10-071.msp>
- * BID: 43696
<http://www.securityfocus.com/bid/43696>
- * VUPEN: VUPEN/ADV-2010-2618
<http://www.vupen.com/english/advisories/2010/2618>
- * SECTRACK: 1024546
<http://securitytracker.com/alerts/2010/Oct/1024546.html>

CVE Reference:

CVE-2010-3326 (cve.mitre.org, nvd.nist.gov)

• 18958 Anchor Element Information Disclosure Vulnerability (MS10-071/2360131) (Remote File Checking)

An information disclosure vulnerability exists in the way that Internet Explorer improperly handles the Anchor element. This behavior occurs during user operation when the Anchor element is not removed during content pasting and editing, potentially revealing personally identifiable information intended for deletion.

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

References:

- * MS: MS10-071
<http://www.microsoft.com/technet/security/bulletin/ms10-071.msp>
- * BID: 43704
<http://www.securityfocus.com/bid/43704>
- * VUPEN: VUPEN/ADV-2010-2618
<http://www.vupen.com/english/advisories/2010/2618>
- * SECTRACK: 1024546
<http://securitytracker.com/alerts/2010/Oct/1024546.html>

CVE Reference:

CVE-2010-3327 (cve.mitre.org, nvd.nist.gov)

• 18959 Uninitialized Memory Corruption Vulnerability (CVE-2010-3328) (MS10-071/2360131) (Remote File Checking)

A remote code execution vulnerability exists in the way that 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: MS10-071
<http://www.microsoft.com/technet/security/bulletin/ms10-071.msp>
- * BID: 43705
<http://www.securityfocus.com/bid/43705>
- * VUPEN: VUPEN/ADV-2010-2618
<http://www.vupen.com/english/advisories/2010/2618>
- * SECTRACK: 1024546
<http://securitytracker.com/alerts/2010/Oct/1024546.html>

CVE Reference:

CVE-2010-3328 (cve.mitre.org, nvd.nist.gov)

• 18960 Uninitialized Memory Corruption Vulnerability (CVE-2010-3329) (MS10-071/2360131) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted when a document in an HTML format is opened in Microsoft Word. An attacker could exploit the vulnerability by convincing the user to open a malicious Word document. When a user closes the document, 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: MS10-071
<http://www.microsoft.com/technet/security/bulletin/ms10-071.msp>
- * BID: 43706
<http://www.securityfocus.com/bid/43706>
- * VUPEN: VUPEN/ADV-2010-2618
<http://www.vupen.com/english/advisories/2010/2618>
- * SECTRACK: 1024546
<http://securitytracker.com/alerts/2010/Oct/1024546.html>

CVE Reference:

CVE-2010-3329 (cve.mitre.org, nvd.nist.gov)

• **18961 Cross-Domain Information Disclosure Vulnerability (MS10-071/2360131) (Remote File Checking)**

An information disclosure vulnerability exists in Internet Explorer that could allow script to gain access to information in another domain or Internet Explorer zone. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow information disclosure if a user viewed the Web page. An attacker who successfully exploited this vulnerability could view content from another domain or Internet Explorer zone.

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

References:

- * MS: MS10-071
<http://www.microsoft.com/technet/security/bulletin/ms10-071.msp>
- * BID: 43709
<http://www.securityfocus.com/bid/43709>
- * VUPEN: VUPEN/ADV-2010-2618
<http://www.vupen.com/english/advisories/2010/2618>
- * SECTRAK: 1024546
<http://securitytracker.com/alerts/2010/Oct/1024546.html>

CVE Reference:

CVE-2010-3330 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2010-1883 Microsoft CVSS 2.0 Score = 9.3**

Integer overflow in the Embedded OpenType (EOT) Font Engine in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows remote attackers to execute arbitrary code via a crafted table in an embedded font, aka "Embedded OpenType Font Integer Overflow Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-076.msp>

CVE Reference: [CVE-2010-1883](#)

• **CVE-2010-2745 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Windows Media Player (WMP) 9 through 12 does not properly deallocate objects during a browser reload action, which allows user-assisted remote attackers to execute arbitrary code via crafted media content referenced in an HTML document, aka "Windows Media Player Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-082.msp>

CVE Reference: [CVE-2010-2745](#)

• **CVE-2010-2747 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Word 2002 SP3 and Office 2004 for Mac do not properly handle an uninitialized pointer during parsing of a Word document, which allows remote attackers to execute arbitrary code via a crafted document that triggers memory corruption, aka "Word Uninitialized Pointer Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-079.msp>

CVE Reference: [CVE-2010-2747](#)

• **CVE-2010-2748 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Word 2002 SP3 and Office 2004 for Mac do not properly check an unspecified boundary during parsing of a Word document, which allows remote attackers to execute arbitrary code via a crafted document that triggers memory corruption, aka "Word Boundary Check Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-079.msp>

CVE Reference: [CVE-2010-2748](#)

• **CVE-2010-2750 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Word 2002 SP3 and Office 2004 for Mac do not properly handle an invalid index value during parsing of a Word document, which allows remote attackers to execute arbitrary code via a crafted document that triggers memory corruption, aka "Word Index Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-079.msp>

CVE Reference: [CVE-2010-2750](#)

• **CVE-2010-3214 Microsoft CVSS 2.0 Score = 9.3**

Stack-based buffer overflow in Microsoft Word 2002 SP3, 2003 SP3, 2007 SP2, and 2010; Office 2004 and 2008 for Mac; Open XML File Format Converter for Mac; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP2; Word Viewer; Office Web Apps; and Word Web App allows remote attackers to execute arbitrary code via a crafted Word document, aka "Word Stack Overflow Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-079.msp>

CVE Reference: [CVE-2010-3214](#)

• **CVE-2010-3215 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Word 2002 SP3 and Office 2004 for Mac do not properly handle unspecified return values during parsing of a Word document, which allows remote attackers to execute arbitrary code via a crafted document that triggers memory corruption, aka "Word Return Value Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-079.msp>

CVE Reference: [CVE-2010-3215](#)

• **CVE-2010-3216 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Word 2002 SP3 and Office 2004 for Mac do not properly handle bookmarks during parsing of a Word document, which allows remote attackers to execute arbitrary code via a crafted document that triggers memory corruption, aka "Word Bookmarks Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-079.msp>

CVE Reference: [CVE-2010-3216](#)

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