

2010 Issue #29

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

Top 15 vulnerabilities. Zeus targeting US Bank customers in phishing attack. See who receives most spam. US Cyber security program needs more work.

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

• Report: Adobe Reader, IE top vulnerability list

These are the top 15 most observed vulnerabilities for the first half of 2010 alongside the year they were disclosed and the year they were patched.

(Credit: M86 Security Labs)

The most exploited vulnerabilities tend to be Adobe Reader and Internet Explorer, but a rising target for exploits is Java, according to a report to be released on Wednesday by M86 Security Labs. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20010473-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• Zeus now spoofing Visa, MasterCard programs

A new configuration of the data stealing trojan Zeus is targeting U.S. banking customers with a phishing exploit that spoofs two programs used by credit card companies to offer enhanced payment protection to online shoppers, according to researchers at security firm Trusteer. The attack, which began last week, affects a subset of Zeus installations, Amit Klein, CTO of Trusteer and head of the company's research group, told SCMagazineUS.com on Wednesday.

After an infected user logs in to one of the approximately 15 affected online banking sites, the trojan injects into the browser a phishing screen that contains logos for "Verified by Visa" and "MasterCard SecureCode," both of which are credit card security programs that allow users to confirm their identity with an extra password when making an online transaction. SC Magazine

Full Story :

http://www.scmagazineus.com/zeus-now-spoofing-visa-mastercard-programs/article/174635/?utm_source=feedburner

• **Engineering, automotive sectors commonly spammed**

Organizations in the engineering, automotive and accommodation sectors receive the most spam, according to a report released Wednesday by Symantec Hosted Services.

With spam accounting for 94.1 percent of all email received, engineering organizations top the charts as the most spammed industry, according to Symantec's annual MessageLabs Intelligence Special Report. The second most spammed industry was automotive, followed by accommodation and catering, with 92.9 percent and 90.5 percent of all email identified as spam, respectively. The least spammed sectors are business support services, general services and finance, each with spam rates around 87 percent.

Across the board, small to midsize businesses (SMBs) receive more spam than large enterprises, according to the report. Areas with large populations of SMBs received the greatest proportion of spam, and the least spammed areas are home to many of the largest companies. SC Magazine

Full Story :

http://www.scmagazineus.com/engineering-automotive-sectors-commonly-spammed/article/174595/?utm_source=feedburner

• **Cyber progress report: More work is needed**

U.S. Cyber Coordinator Howard Schmidt presented a cybersecurity progress report Wednesday at the White House, a meeting at which industry and government leaders agreed that more work needs to be done and public- and private-sector partnerships must be strengthened. One of those in attendance, Larry Clinton, president of the Internet Security Alliance (ISA), told SCMagazineUS.com on Thursday that those from the government seemed proud of the progress that has been made on cybersecurity, but agreed that more work is needed.

"Howard Schmidt started the meeting by basically saying the "status quo is unacceptable," Clinton said. During his talk, Schmidt also spoke about the need to make it more costly for cybercriminals to commit offenses.

Meanwhile, President Obama spoke at the meeting for about 10 minutes. SC Magazine

Full Story :

http://www.scmagazineus.com/cyber-progress-report-more-work-is-needed/article/174692/?utm_source=feedburner

New Vulnerabilities Tested in SecureScout

• **14584 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-2201) (Remote File Checking)**

Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code via a PDF file with crafted Flash content involving the (1) pushstring (0x2C) operator, (2) debugfile (0xF1) operator, and an "invalid pointer vulnerability" that triggers memory corruption, a different vulnerability than CVE-2010-1285 and CVE-2010-2168.

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

References:

* BUGTRAQ: 20100630 VUPEN Security Research - Adobe Acrobat and Reader "pushstring" Memory Corruption Vulnerability (CVE-2010-2201)

<http://www.securityfocus.com/archive/1/512098>

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb10-15.html>

* BID: 41237

<http://www.securityfocus.com/bid/41237>

CVE Reference:

CVE-2010-2201 (cve.mitre.org, nvd.nist.gov)

• 14585 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-2202) (Remote File Checking)

Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-1295, CVE-2010-2207, CVE-2010-2209, CVE-2010-2210, CVE-2010-2211, and CVE-2010-2212.

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

References:

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb10-15.html>

* BID: 41234

<http://www.securityfocus.com/bid/41234>

* SECTRACK: 1024159

<http://securitytracker.com/alerts/2010/Jun/1024159.html>

* VUPEN: VUPEN/ADV-2010-1636

<http://www.vupen.com/english/advisories/2010/1636>

CVE Reference:

CVE-2010-2202 (cve.mitre.org, nvd.nist.gov)

• 14586 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-2204) (Remote File Checking)

Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors.

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

References:

* SECTRACK: 1024159

<http://securitytracker.com/alerts/2010/Jun/1024159.html>

* VUPEN: VUPEN/ADV-2010-1636

<http://www.vupen.com/english/advisories/2010/1636>

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb10-15.html>

* BID: 41231

<http://www.securityfocus.com/bid/41231>

CVE Reference:

CVE-2010-2204 (cve.mitre.org, nvd.nist.gov)

• 14587 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-2205) (Remote File Checking)

Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, access uninitialized memory, which allows attackers to execute arbitrary code via unspecified vectors.

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

References:

* SECTRACK: 1024159

<http://securitytracker.com/alerts/2010/Jun/1024159.html>

* VUPEN: VUPEN/ADV-2010-1636

<http://www.vupen.com/english/advisories/2010/1636>

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb10-15.html>

* BID: 41238

<http://www.securityfocus.com/bid/41238>

CVE Reference:

CVE-2010-2205 (cve.mitre.org, nvd.nist.gov)

● **14588 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-2206) (Remote File Checking)**

Array index error in AcroForm.api in Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allows remote attackers to execute arbitrary code via a crafted GIF image in a PDF file, which bypasses a size check and triggers a heap-based buffer overflow.

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

References:

* SECTRACK: 1024159

<http://securitytracker.com/alerts/2010/Jun/1024159.html>

* VUPEN: VUPEN/ADV-2010-1636

<http://www.vupen.com/english/advisories/2010/1636>

* BID: 41238

<http://www.securityfocus.com/bid/41238>

* BUGTRAQ: 20100630 Secunia Research: Adobe Reader GIF Image Parsing Array-Indexing Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/512092/100/0/threaded>

* MISC:

http://secunia.com/secunia_research/2010-88/

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb10-15.html>

* BID: 41241

<http://www.securityfocus.com/bid/41241>

CVE Reference:

CVE-2010-2206 (cve.mitre.org, nvd.nist.gov)

● **18850 Access ActiveX Control Vulnerability (MS10-044/982335) (Remote File Checking)**

A remote code execution vulnerability exists in Access ActiveX controls due to the way that multiple ActiveX controls are loaded by Internet Explorer. An attacker who successfully exploited this vulnerability could run arbitrary code as the logged-on user. If a user is logged on with administrative user rights, an attacker could take complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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: MS10-044

<http://www.microsoft.com/technet/security/bulletin/MS10-044.mspx>

* BID: 41442

<http://www.securityfocus.com/bid/41442>

* SECTRACK: 1024188

<http://securitytracker.com/alerts/2010/Jul/1024188.html>

* VUPEN: VUPEN/ADV-2010-1799

<http://www.vupen.com/english/advisories/2010/1799>

CVE Reference:

CVE-2010-0814 (cve.mitre.org, nvd.nist.gov)

● **18851 ACCWIZ.dll Uninitialized Variable Vulnerability (MS10-044/982335) (Remote File Checking)**

A remote code execution vulnerability exists in the way that the FieldList ActiveX control is instantiated by Microsoft Office and Internet Explorer. An attacker who successfully exploited this vulnerability could run arbitrary code as the logged-on user. If a user is logged on with administrative user rights, an attacker could take complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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: MS10-044

<http://www.microsoft.com/technet/security/bulletin/MS10-044.mspx>

* BID: 41444

<http://www.securityfocus.com/bid/41444>

* SECTRACK: 1024188

<http://securitytracker.com/alerts/2010/Jul/1024188.html>

* VUPEN: VUPEN/ADV-2010-1799

<http://www.vupen.com/english/advisories/2010/1799>

CVE Reference:

CVE-2010-1881 (cve.mitre.org, nvd.nist.gov)

• 18852 Microsoft Outlook SMB Attachment Vulnerability (MS10-045/978212) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Outlook verifies attachments in a specially crafted e-mail message. 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: MS10-045

<http://www.microsoft.com/technet/security/bulletin/MS10-045.msp>

* BID: 41446

<http://www.securityfocus.com/bid/41446>

* SECTRACK: 1024189

<http://securitytracker.com/alerts/2010/Jul/1024189.html>

* VUPEN: VUPEN/ADV-2010-1800

<http://www.vupen.com/english/advisories/2010/1800>

CVE Reference:

CVE-2010-0266 (cve.mitre.org, nvd.nist.gov)

• 18853 Canonical Display Driver Integer Overflow Vulnerability (MS10-043/2032276) (Remote File Checking)

An unauthenticated remote code execution vulnerability exists in the way that the Microsoft Canonical Display Driver (cdd.dll) parses information copied from user mode to kernel mode. Although it is possible that the vulnerability could allow code execution, successful code execution is unlikely due to memory randomization. In most scenarios, it is much more likely that an attacker who successfully exploited this vulnerability could cause the affected system to stop responding and automatically restart. An attacker who can successfully exploit this vulnerability for code execution could execute arbitrary code and 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: MS10-043

<http://www.microsoft.com/technet/security/bulletin/MS10-043.msp>

* BID: 40237

<http://www.securityfocus.com/bid/40237>

* SECTRACK: 1023991

<http://securitytracker.com/alerts/2010/May/1023991.html>

* VUPEN: VUPEN/ADV-2010-1178

<http://www.vupen.com/english/advisories/2010/1178>

CVE Reference:

CVE-2009-3678 (cve.mitre.org, nvd.nist.gov)

• 18854 Help Center URL Validation Vulnerability (MS10-042/2229593) (Remote File Checking)

An unauthenticated remote code execution vulnerability exists in the way that the Microsoft Help and Support Center validates specially crafted URLs. This vulnerability could allow remote code execution if a user views a specially crafted Web page using a Web browser or clicks a specially crafted link in an e-mail message. An attacker who successfully exploited this vulnerability could execute arbitrary code and 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: MS10-042

<http://www.microsoft.com/technet/security/bulletin/MS10-042.msp>

* BID: 40725

<http://www.securityfocus.com/bid/40725>

* SECTRACK: 1024084

<http://securitytracker.com/alerts/2010/Jun/1024084.html>

* VUPEN: VUPEN/ADV-2010-1417

<http://www.vupen.com/english/advisories/2010/1417>

CVE Reference:

CVE-2010-1885 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-0873 Oracle CVSS 2.0 Score = 10.0

Unspecified vulnerability in the Data Server component in Oracle TimesTen In-Memory Database 7.0.6.0 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

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

References:

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuijul2010.html>

CVE Reference: [CVE-2010-0873](#)

• CVE-2010-0898 Oracle CVSS 2.0 Score = 10.0

Unspecified vulnerability in Oracle Secure Backup 10.3.0.1 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

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

References:

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuijul2010.html>

CVE Reference: [CVE-2010-0898](#)

• CVE-2010-0907 Oracle CVSS 2.0 Score = 10.0

Unspecified vulnerability in Oracle Secure Backup 10.3.0.1 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2010-0898, CVE-2010-0899, CVE-2010-0904, and CVE-2010-0906.

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

References:

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuijul2010.html>

CVE Reference: [CVE-2010-0907](#)

• CVE-2010-0899 Oracle CVSS 2.0 Score = 9.0

Unspecified vulnerability in Oracle Secure Backup 10.3.0.1 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2010-0898, CVE-2010-0907, and CVE-2010-0906.

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

References:

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuijul2010.html>

CVE Reference: [CVE-2010-0899](#)

• CVE-2010-0906 Oracle CVSS 2.0 Score = 9.0

Unspecified vulnerability in Oracle Secure Backup 10.3.0.1 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors.

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

References:

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuijul2010.html>

CVE Reference: [CVE-2010-0906](#)

• **CVE-2010-0903 Oracle CVSS 2.0 Score = 7.8**

Unspecified vulnerability in the Net Foundation Layer component in Oracle Database Server 9.2.0.8, 10.1.0.5, 10.2.0.4, 11.1.0.7, and 11.2.0.1, when running on Windows, allows remote attackers to affect availability via unknown vectors.

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

References:

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuijul2010.html>

CVE Reference: [CVE-2010-0903](#)

• **CVE-2010-0911 Oracle CVSS 2.0 Score = 7.8**

Unspecified vulnerability in the Listener component in Oracle Database Server 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.4, 11.1.0.7, and 11.2.0.1 allows remote attackers to affect availability via unknown vectors.

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

References:

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuijul2010.html>

CVE Reference: [CVE-2010-0911](#)

• **CVE-2010-0083 Oracle CVSS 2.0 Score = 7.6**

Unspecified vulnerability in Oracle OpenSolaris 8, 9, and 10 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

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

References:

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuijul2010.html>

CVE Reference: [CVE-2010-0083](#)

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