

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

Time for next year predictions. SQL injection used to access bank cards. hackers against human rights and free speech.

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

• 10 IT-related predictions for 2011

IDG News Service - We were wrong -- so far -- that Carol Bartz would be ousted as Yahoo CEO by the end of this year, but we were right that Apple's tablet, whose name wasn't known at the end of last year, would be huge. OK, so that second one was probably a given, but not all of our 2010 predictions were so easy. We think the same is true with our 2011 predictions.

Sometimes a cliché works best Computerworld

Full Story :

http://www.computerworld.com/s/article/9201720/10_IT_related_predictions_for_2011?source=rss_security

• Hackers hit New York tour firm, access 110,000 bank cards

IDG News Service - Hackers have broken into the website of the New York tour company CitySights NY and stolen about 110,000 bank card numbers.

They broke in using a SQL Injection attack on the company's Web server, CitySights NY said in a Dec. 9 breach notification letter published by New Hampshire's attorney general. The company learned of the problem in late October, when, "a web programmer discovered [an] unauthorized script that appears to have been uploaded to the company's web server, which is believed to have compromised the security of the database on that server," the letter said.

CitySights NY believes that the SQL injection compromise occurred about a month earlier, on Sept. 26. In a SQL injection attack, hackers find ways to sneak real database commands into the server using the Web. They do this by adding specially crafted text into Web-based forms or search boxes that are used to query the back-end database.
Computerworld

Full Story :

http://www.computerworld.com/s/article/9201822/Hackers_hit_New_York_tour_firm_access_110_00_bank_cards?so

• DDoS attacks threaten free speech, says report

Computerworld - Computer attacks launched against sites run by human rights and dissident media groups threaten to knock free speech off the Web, a new report warned this week.

The study conducted by Harvard University's Berkman Center for Internet & Society showed that distributed denial-of-service (DDoS) attacks frequently knocked such sites offline.

Of the sites surveyed by the center, 62% were victimized by DDoS attacks in the last 12 months, and 61% experienced unexplained downtime. Computerworld

Full Story :

http://www.computerworld.com/s/article/9202138/DDoS_attacks_threaten_free_speech_says_report?source=rss_sec

• Hackers targeting human rights, indie media groups

Hackers are increasingly hitting the Web sites of human rights and independent media groups in an attempt to silence them, says a new study released this week by Harvard University's Berkman Center for Internet & Society.

Based on a survey of 45 groups, the report "Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites" found that a large percentage said they've been targeted by distributed denial-of-service (DDoS) attacks from those who disagree with their viewpoints. The Web sites typically have been knocked offline for short periods of time but in some cases have been down for days.

(Credit: Berkman Center for Internet & Society) Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20026516-83.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 19104 Size Value Heap Corruption in pubconv.dll Vulnerability (MS10-103/2292970) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Publisher parses Publisher files. An attacker could exploit the vulnerability by creating a specially crafted Publisher file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site, and then convincing the user to open the specially crafted Publisher file. If a user were 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

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

References:

* VUPEN: VUPEN/ADV-2010-3225

<http://www.vupen.com/english/advisories/2010/3225>

* BID: 45277

<http://www.securityfocus.com/bid/45277>

* MS: MS10-103

<http://www.microsoft.com/technet/security/Bulletin/MS10-103.msp>

* SECTRACK: 1024885

<http://securitytracker.com/id?1024885>

CVE Reference:

CVE-2010-2569 (cve.mitre.org, nvd.nist.gov)

• 19105 Heap Overrun in pubconv.dll Vulnerability (MS10-103/2292970) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Publisher parses Publisher files. An attacker could exploit the vulnerability by creating a specially crafted Publisher file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site, and then convincing the user to open the specially crafted Publisher file. If a user were 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

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

References:

* VUPEN: VUPEN/ADV-2010-3225

<http://www.vupen.com/english/advisories/2010/3225>

* BID: 45279

<http://www.securityfocus.com/bid/45279>

* MS: MS10-103

<http://www.microsoft.com/technet/security/Bulletin/MS10-103.msp>

* SECTRACK: 1024885

<http://securitytracker.com/id?1024885>

CVE Reference:

CVE-2010-2570 (cve.mitre.org, nvd.nist.gov)

• 19106 Memory Corruption Due To Invalid Index Into Array in Pubconv.dll Vulnerability (MS10-103/2292970) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Publisher opens Publisher files. An attacker could exploit the vulnerability by creating a specially crafted Publisher file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site, and then convincing the user to open the specially crafted Publisher file. If a user were 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

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

References:

* VUPEN: VUPEN/ADV-2010-3225

<http://www.vupen.com/english/advisories/2010/3225>

* BID: 45280

<http://www.securityfocus.com/bid/45280>

* MS: MS10-103

<http://www.microsoft.com/technet/security/Bulletin/MS10-103.msp>

* SECTRACK: 1024885

<http://securitytracker.com/id?1024885>

CVE Reference:

CVE-2010-2571 (cve.mitre.org, nvd.nist.gov)

• 19107 Microsoft Publisher Memory Corruption Vulnerability (MS10-103/2292970) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Publisher opens Publisher files. An attacker could exploit the vulnerability by creating a specially crafted Publisher file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site, and then convincing the user to open the specially crafted Publisher file. If a user were 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

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

References:

* VUPEN: VUPEN/ADV-2010-3225
<http://www.vupen.com/english/advisories/2010/3225>
* BID: 45281
<http://www.securityfocus.com/bid/45281>
* MS: MS10-103
<http://www.microsoft.com/technet/security/Bulletin/MS10-103.aspx>
* SECTRACK: 1024885
<http://securitytracker.com/id?1024885>

CVE Reference:

CVE-2010-3954 (cve.mitre.org, nvd.nist.gov)

• **19108 Array Indexing Memory Corruption Vulnerability (MS10-103/2292970) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Publisher opens Publisher files. An attacker could exploit the vulnerability by creating a specially crafted Publisher file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site, and then convincing the user to open the specially crafted Publisher file. If a user were 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

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

References:

* VUPEN: VUPEN/ADV-2010-3225
<http://www.vupen.com/english/advisories/2010/3225>
* BID: 45282
<http://www.securityfocus.com/bid/45282>
* MS: MS10-103
<http://www.microsoft.com/technet/security/Bulletin/MS10-103.aspx>
* SECTRACK: 1024885
<http://securitytracker.com/id?1024885>

CVE Reference:

CVE-2010-3955 (cve.mitre.org, nvd.nist.gov)

• **19109 Win32k Buffer Overflow Vulnerability (MS10-098/2436673) (Remote File Checking)**

An elevation of privilege vulnerability exists in the way that Windows kernel-mode drivers improperly allocate memory when copying data from user mode. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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:

* VUPEN: VUPEN/ADV-2010-3220
<http://www.vupen.com/english/advisories/2010/3220>
* SECTRACK: 1024880
<http://www.securitytracker.com/id?1024880>
* MS: MS10-098
<http://www.microsoft.com/technet/security/Bulletin/MS10-098.aspx>

CVE Reference:

CVE-2010-3939 (cve.mitre.org, nvd.nist.gov)

• **19110 Win32k PFE Pointer Double Free Vulnerability (MS10-098/2436673) (Remote File Checking)**

An elevation of privilege vulnerability exists due to the way that the Windows kernel-mode drivers free objects that are no longer in use. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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:

* VUPEN: VUPEN/ADV-2010-3220
<http://www.vupen.com/english/advisories/2010/3220>

* SECTRACK: 1024880

<http://www.securitytracker.com/id?1024880>

* MS: MS10-098

<http://www.microsoft.com/technet/security/Bulletin/MS10-098.msp>

* BID: 45286

<http://www.securityfocus.com/bid/45286>

CVE Reference:

CVE-2010-3940 (cve.mitre.org, nvd.nist.gov)

• 19111 Win32k Double Free Vulnerability (MS10-098/2436673) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that the Windows kernel-mode drivers free objects that are no longer in use. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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:

* VUPEN: VUPEN/ADV-2010-3220

<http://www.vupen.com/english/advisories/2010/3220>

* SECTRACK: 1024880

<http://www.securitytracker.com/id?1024880>

* MS: MS10-098

<http://www.microsoft.com/technet/security/Bulletin/MS10-098.msp>

* BID: 45287

<http://www.securityfocus.com/bid/45287>

CVE Reference:

CVE-2010-3941 (cve.mitre.org, nvd.nist.gov)

• 19112 Win32k WriteAV Vulnerability (MS10-098/2436673) (Remote File Checking)

An elevation of privilege vulnerability exists in the way that Windows kernel-mode drivers improperly allocate memory when copying data from user mode. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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:

* VUPEN: VUPEN/ADV-2010-3220

<http://www.vupen.com/english/advisories/2010/3220>

* SECTRACK: 1024880

<http://www.securitytracker.com/id?1024880>

* MS: MS10-098

<http://www.microsoft.com/technet/security/Bulletin/MS10-098.msp>

* BID: 45288

<http://www.securityfocus.com/bid/45288>

CVE Reference:

CVE-2010-3942 (cve.mitre.org, nvd.nist.gov)

• 19113 Win32k Cursor Linking Vulnerability (MS10-098/2436673) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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:

* VUPEN: VUPEN/ADV-2010-3220

<http://www.vupen.com/english/advisories/2010/3220>

* SECTRACK: 1024880

<http://www.securitytracker.com/id?1024880>

* MS: MS10-098

<http://www.microsoft.com/technet/security/Bulletin/MS10-098.msp>

* BID: 45289

<http://www.securityfocus.com/bid/45289>

CVE Reference:

CVE-2010-3943 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2010-3970 Microsoft CVSS 2.0 Score = 10.0**

Unspecified vulnerability in Microsoft Windows has unknown impact and attack vectors, as reported by Moti and Xu Hao.

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

References:

MISC: <http://www.powerofcommunity.net/speaker.html>

CVE Reference: [CVE-2010-3970](http://cve.mitre.org/cve/2010/3970)

• **CVE-2010-3972 Microsoft CVSS 2.0 Score = 10.0**

The TELNET_STREAM_CONTEXT::OnSendData function in the FTP protocol handler (ftpsvc.dll) for Microsoft Internet Information Services (IIS) 7.5 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted FTP request that triggers memory corruption. NOTE: some of these details are obtained from third party information.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/64248>

VUPEN: <http://www.vupen.com/english/advisories/2010/3305>

BID: <http://www.securityfocus.com/bid/45542>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/15803>

SECUNIA: <http://secunia.com/advisories/42713>

CVE Reference: [CVE-2010-3972](http://cve.mitre.org/cve/2010/3972)

• **CVE-2010-3971 Microsoft CVSS 2.0 Score = 9.3**

Use-after-free vulnerability in the CSharedStyleSheet::Notify function in the Cascading Style Sheets (CSS) parser in mshtml.dll, as used in Microsoft Internet Explorer 7 and 8 and possibly other products, allows remote attackers to cause a denial of service (crash) and execute arbitrary code via multiple @import calls in a crafted document.

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

References:

MISC: <http://www.wooyun.org/bugs/wooyun-2010-0885>

VUPEN: <http://www.vupen.com/english/advisories/2010/3156>

BID: <http://www.securityfocus.com/bid/45246>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/15746>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/15708>

MISC: <http://www.breakingpointsystems.com/community/blog/ie-vulnerability/>

SECUNIA: <http://secunia.com/advisories/42510>

FULLDISC: <http://seclists.org/fulldisclosure/2010/Dec/110>

CVE Reference: [CVE-2010-3971](http://cve.mitre.org/cve/2010/3971)

• **CVE-2010-3973 Microsoft CVSS 2.0 Score = 9.3**

The WBEMSingleView.ocx ActiveX control 1.50.1131.0 in Microsoft WMI Administrative Tools 1.1 and earlier allows remote attackers to execute arbitrary code via a crafted argument to the AddContextRef method, possibly an untrusted pointer dereference.

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

References:

CERT-VN: <http://www.kb.cert.org/vuls/id/725596>

XF: <http://xforce.iss.net/xforce/xfdb/64250>

MISC: <http://www.wooyun.org/bug.php?action=view&id=1006>

VUPEN: <http://www.vupen.com/english/advisories/2010/3301>

BID: <http://www.securityfocus.com/bid/45546>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/15809>

SECUNIA: <http://secunia.com/advisories/42693>

CVE Reference: [CVE-2010-3973](#)

• **CVE-2010-4588 Microsoft CVSS 2.0 Score = 9.3**

The WBEMSingleView.ocx ActiveX control 1.50.1131.0 in Microsoft WMI Administrative Tools 1.1 and earlier allows remote attackers to execute arbitrary code via a crafted argument to the ReleaseContext method, a different vector than CVE-2010-3973, possibly an untrusted pointer dereference.

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

References:

CERT-VN: <http://www.kb.cert.org/vuls/id/725596>

MISC: <http://www.wooyun.org/bug.php?action=view&id=1006>

MISC: <http://twitter.com/carsteneiram/status/17526155733110784>

SECUNIA: <http://secunia.com/advisories/42693>

CVE Reference: [CVE-2010-4588](#)

• **CVE-2010-4116 HP CVSS 2.0 Score = 10.0**

Unspecified vulnerability in HP StorageWorks Storage Mirroring 5.x before 5.2.2.1771.2 allows remote attackers to execute arbitrary code via unknown vectors.

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

References:

SECUNIA: <http://secunia.com/advisories/42696>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02660122>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02660122>

CVE Reference: [CVE-2010-4116](#)

• **CVE-2010-4113 HP CVSS 2.0 Score = 9.3**

Unspecified vulnerability in HP Power Manager (HPPM) before 4.3.2 allows remote attackers to execute arbitrary code via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=129251322532373&w=2>

HP: <http://marc.info/?l=bugtraq&m=129251322532373&w=2>

CVE Reference: [CVE-2010-4113](#)

• **CVE-2010-4110 HP CVSS 2.0 Score = 5.7**

Unspecified vulnerability in HP OpenVMS 8.3, 8.3-1H1, and 8.4 on the Itanium platform on Integrity servers allows local users to gain privileges or cause a denial of service via unknown vectors.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/3247>

BID: <http://www.securityfocus.com/bid/45416>

SECUNIA: <http://secunia.com/advisories/42610>

HP: <http://marc.info/?l=bugtraq&m=129243663611240&w=2>

HP: <http://marc.info/?l=bugtraq&m=129243663611240&w=2>

CVE Reference: [CVE-2010-4110](#)

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