

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

Spoofed youtube with malware. Spoofed Twitter emails with malware. iPad user information exposed. Massive SQL attack.

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

• Scores of spoofed YouTube pages lead to malware

Researchers at network security firm eSoft on Wednesday discovered more than 700,000 web pages crafted to look identical to YouTube but which are spreading malware.

The malicious pages claim to contain a "hot video" associated with the Gulf oil spill, NBA Playoffs, Harry Potter and other popular topics, Patrick Walsh, CTO at eSoft, told SCMagazineUS.com on Wednesday. The spoofed pages appear legitimate and even contain a YouTube logo.

Attempting to play the video on one of the bogus pages causes a pop-up to appear informing users they need to download and install a media codec, Lee Graves, threat communications specialist at eSoft, told SCMagazineUS.com on Wednesday. Clicking "OK" to install the codec causes a user's browser to be redirected through several intermediary sites before landing on a final malware distribution site. SC Magazine

Full Story :

http://www.scmagazineus.com/scores-of-spoofed-youtube-pages-lead-to-malware/article/172043/?utm_source=feed

• Spam masquerading as Twitter e-mails lead to phishing, malware

The spam appears to come from the Twitter customer support team.

(Credit: Trend Micro)

E-mail inboxes are getting hit this week with spam campaigns that appear to be legitimate Twitter messages but which lead to malware and phishing sites, security firms warned on Wednesday. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20007246-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• AT&T Web site exposes data of 114,000 iPad users

A group of hackers exploited a hole in an AT&T Web site to get e-mail addresses of about 114,000 iPad users, including what appears to be top officials in government, finance, media, technology, and military.

The leak could have affected all iPad 3G subscribers in the U.S., according to Gawker, which broke the story on Wednesday. Among the iPad users who appeared to have been affected were White House Chief of Staff Rahm Emanuel, Diane Sawyer, New York Mayor Michael Bloomberg, movie producer Harvey Weinstein, and New York Times CEO Janet Robinson. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20007309-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• Wall Street Journal, others, hit in mass SQL attack

Security researchers have discovered a widescale SQL injection attack that has compromised thousands of websites to spread malware, including pages belonging to the Wall Street Journal and the Jerusalem Post. The sites were injected with HTML code that attempted to load malware from a malicious web server - robint.us - onto visitors' PCs, researchers said. All of the affected sites are hosted on Microsoft Internet Information Services (IIS) web servers, and are using Active Server Pages software from ASP.net, David Dede, lead security researcher at malware detection solutions provider Sucuri Security, told SCMagazineUS.com on Thursday. The attacks, however, are the result of vulnerabilities in third-party web applications and do not demonstrate holes in Microsoft software, Microsoft has said.

"Looking at the logs, the attackers were scanning for multiple vulnerabilities, trying different SQL injections," Dede said. SC Magazine

Full Story :

http://www.scmagazineus.com/wall-street-journal-others-hit-in-mass-sql-attack/article/172153/?utm_source=feedburn

New Vulnerabilities Tested in SecureScout

• 18818 Internet Explorer Cross-Domain Information Disclosure Vulnerability (MS10-035/982381) (Remote File Checking)

An information disclosure vulnerability exists in the way that Internet Explorer caches data and incorrectly allows the cached content to be called, potentially bypassing Internet Explorer domain restriction. 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 the local computer or a browser window in another domain or Internet Explorer zone.

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

References:

* BUGTRAQ: 20100203 CORE-2009-0625: Internet Explorer Dynamic OBJECT tag and URLMON sniffing vulnerabilities

<http://www.securityfocus.com/archive/1/archive/1/509345/100/0/threaded>

* MISC:

<http://isc.sans.org/diary.html?n&storyid=8152>

* MISC:

<http://www.coresecurity.com/content/internet-explorer-dynamic-object-tag>

* CONFIRM:

<http://blogs.technet.com/msrc/archive/2010/02/03/security-advisory-980088-released.aspx>

* CONFIRM:

<http://www.microsoft.com/technet/security/advisory/980088.msp>

* MS: MS10-035

<http://www.microsoft.com/technet/security/bulletin/ms10-035.msp>

* CERT: TA10-159B

<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

* BID: 38055

<http://www.securityfocus.com/bid/38055>

* BID: 38056

<http://www.securityfocus.com/bid/38056>

* OSVDB: 62156

<http://osvdb.org/62156>

* VUPEN: VUPEN/ADV-2010-1392

<http://www.vupen.com/english/advisories/2010/1392>

* SECTRACK: 1023542

<http://securitytracker.com/alerts/2010/Feb/1023542.html>

CVE Reference:

CVE-2010-0255 (cve.mitre.org, nvd.nist.gov)

• 18819 Internet Explorer toStaticHTML Information Disclosure Vulnerability (MS10-035/982381) (Remote File Checking)

An information disclosure vulnerability exists in the way that Internet Explorer handles content using specific strings when sanitizing HTML. 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 inflict cross-site scripting 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: **High**

References:

* VUPEN: VUPEN/ADV-2010-1392

<http://www.vupen.com/english/advisories/2010/1392>

* SECTRACK: 1024068

<http://securitytracker.com/alerts/2010/Jun/1024068.html>

* MS: MS10-035

<http://www.microsoft.com/technet/security/bulletin/ms10-035.msp>

* MS: MS10-039

<http://www.microsoft.com/technet/security/bulletin/ms10-039.msp>

* CERT: TA10-159B

<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

* BID: 40409

<http://www.securityfocus.com/bid/40409>

CVE Reference:

CVE-2010-1257 (cve.mitre.org, nvd.nist.gov)

• 18820 Internet Explorer Uninitialized Memory Corruption Vulnerability (CVE-2010-1259) (MS10-035/982381) (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:

* VUPEN: VUPEN/ADV-2010-1392

<http://www.vupen.com/english/advisories/2010/1392>

* SECTRACK: 1024068

<http://securitytracker.com/alerts/2010/Jun/1024068.html>

* BID: 40410

<http://www.securityfocus.com/bid/40410>

* MS: MS10-035

<http://www.microsoft.com/technet/security/bulletin/ms10-035.msp>

* CERT: TA10-159B

<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

CVE Reference:

CVE-2010-1259 (cve.mitre.org, nvd.nist.gov)

• **18821 Internet Explorer HTML Element Memory Corruption Vulnerability (MS10-035/982381) (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 in the IE8 Developer Toolbar. 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:

- * VUPEN: VUPEN/ADV-2010-1392
<http://www.vupen.com/english/advisories/2010/1392>
- * SECTRACK: 1024068
<http://securitytracker.com/alerts/2010/Jun/1024068.html>
- * BID: 40414
<http://www.securityfocus.com/bid/40414>
- * MS: MS10-035
<http://www.microsoft.com/technet/security/bulletin/ms10-035.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

CVE Reference:

CVE-2010-1260 (cve.mitre.org, nvd.nist.gov)

• **18822 Internet Explorer Uninitialized Memory Corruption Vulnerability (CVE-2010-1261) (MS10-035/982381) (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 in the IE8 Developer Toolbar. 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:

- * VUPEN: VUPEN/ADV-2010-1392
<http://www.vupen.com/english/advisories/2010/1392>
- * SECTRACK: 1024068
<http://securitytracker.com/alerts/2010/Jun/1024068.html>
- * BID: 40416
<http://www.securityfocus.com/bid/40416>
- * MS: MS10-035
<http://www.microsoft.com/technet/security/bulletin/ms10-035.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

CVE Reference:

CVE-2010-1261 (cve.mitre.org, nvd.nist.gov)

• **18823 Internet Explorer Memory Corruption Vulnerability (MS10-035/982381) (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:

- * VUPEN: VUPEN/ADV-2010-1392
<http://www.vupen.com/english/advisories/2010/1392>
- * SECTRACK: 1024068
<http://securitytracker.com/alerts/2010/Jun/1024068.html>
- * BID: 40417
<http://www.securityfocus.com/bid/40417>
- * MS: MS10-035
<http://www.microsoft.com/technet/security/bulletin/ms10-035.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

CVE Reference:

CVE-2010-1262 (cve.mitre.org, nvd.nist.gov)

• 18824 Win32k Improper Data Validation Vulnerability (MS10-032/979559) (Remote File Checking)

An elevation of privilege vulnerability exists because the Windows kernel-mode drivers do not properly validate changes in certain kernel 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-2010-1389
<http://www.vupen.com/english/advisories/2010/1389>
- * SECTRACK: 1024072
<http://securitytracker.com/alerts/2010/Jun/1024072.html>
- * BID: 40508
<http://www.securityfocus.com/bid/40508>
- * MS: MS10-032
<http://www.microsoft.com/technet/security/bulletin/ms10-032.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

CVE Reference:

CVE-2010-0484 (cve.mitre.org, nvd.nist.gov)

• 18825 Win32k Window Creation Vulnerability (MS10-032/979559) (Remote File Checking)

An elevation of privilege vulnerability exists because Windows kernel-mode drivers do not properly validate all parameters when creating a new window. 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-2010-1389
<http://www.vupen.com/english/advisories/2010/1389>
- * SECTRACK: 1024072
<http://securitytracker.com/alerts/2010/Jun/1024072.html>
- * BID: 40569
<http://www.securityfocus.com/bid/40569>
- * MS: MS10-032
<http://www.microsoft.com/technet/security/bulletin/ms10-032.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

CVE Reference:

CVE-2010-0485 (cve.mitre.org, nvd.nist.gov)

• 18826 Win32k TrueType Font Parsing Vulnerability (MS10-032/979559) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that the operating system provides font-related information to applications. 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-2010-1389
<http://www.vupen.com/english/advisories/2010/1389>
- * SECTRACK: 1024072
<http://securitytracker.com/alerts/2010/Jun/1024072.html>
- * BID: 40570
<http://www.securityfocus.com/bid/40570>
- * MS: MS10-032
<http://www.microsoft.com/technet/security/bulletin/ms10-032.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

CVE Reference:

CVE-2010-1255 (cve.mitre.org, nvd.nist.gov)

• 18827 OpenType CFF Font Driver Memory Corruption Vulnerability (MS10-032/979559) (Remote File Checking)

An elevation of privilege vulnerability exists in the Windows OpenType Compact Font Format (CFF) driver due to improper validation of certain data passed from user mode to kernel 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-2010-1394
<http://www.vupen.com/english/advisories/2010/1394>
- * SECTRACK: 1024074
<http://securitytracker.com/alerts/2010/Jun/1024074.html>
- * BID: 40572
<http://www.securityfocus.com/bid/40572>
- * MS: MS10-037
<http://www.microsoft.com/technet/security/bulletin/ms10-037.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

CVE Reference:

CVE-2010-0819 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-1962 HP CVSS 2.0 Score = 10.0

Unspecified vulnerability in HP StorageWorks Storage Mirroring 5 before 5.2.1.870.0 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=127557820805729&w=2>

CVE Reference: [CVE-2010-1962](http://cve.mitre.org/cve/2010/1962)

• CVE-2010-1963 HP CVSS 2.0 Score = 4.3

Cross-site scripting (XSS) vulnerability in HP ServiceCenter allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=127557884206863&w=2>

CVE Reference: [CVE-2010-1963](http://cve.mitre.org/cve/2010/1963)

• **CVE-2010-1439 redhat CVSS 2.0 Score = 3.6**

yum-rhn-plugin in Red Hat Network Client Tools (aka rhn-client-tools) on Red Hat Enterprise Linux (RHEL) 5 and Fedora uses world-readable permissions for the /var/spool/up2date/loginAuth.pkl file, which allows local users to access the Red Hat Network profile, and possibly prevent future security updates, by leveraging authentication data from this file.

Test Case Impact: Vulnerability Impact: Risk: **Low**

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=585386

XF: <http://xforce.iss.net/xforce/xfdb/59114>

VUPEN: <http://www.vupen.com/english/advisories/2010/1311>

BID: <http://www.securityfocus.com/bid/40492>

REDHAT: <http://www.redhat.com/support/errata/RHSA-2010-0449.html>

OSVDB: <http://www.osvdb.org/65063>

SECTRACK: <http://securitytracker.com/id?1024049>

SECUNIA: <http://secunia.com/advisories/39996>

CVE Reference: [CVE-2010-1439](#)

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