

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

SQL injections the highest risk. McAfee update causes problems. IE8 XSS to be fixed. New Zeus targeting online banking.

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

• Injection tops list of web application security risks

Injection flaws, particularly of the SQL kind, are now the most critical web application security risk for enterprises, according to a newly-updated report from the Open Web Application Security Project (OWASP).

The nonprofit open-source application security community on Monday released a new version of its Top 10 list of critical web application security risks, a ranking intended to help organizations better secure their web applications and services.

The OWASP Top 10 list, last updated in 2007, now places a greater emphasis on risks, in addition to vulnerabilities, according to the report. SC Magazine

Full Story :

http://www.scmagazineus.com/injection-tops-list-of-web-application-security-risks/article/168304/?utm_source=feed

• McAfee error wreaks havoc on corporate systems

PCs in organizations around the world were crippled by a flawed McAfee update that caused computers to become stuck in an endless cycle of reboots. The issue began on Wednesday around 9:00 a.m. ET when the security giant pushed out a new virus definition file to PCs running McAfee VirusScan Enterprise. In the release, a legitimate Windows operating system file called "svchost.exe" had somehow been falsely classified as a virus called "W32/Wecorl.a." The faulty update caused computers running Windows XP Service Pack 3 to display a false positive error message or a blue screen and to repeatedly reboot.

Every affected computer will need to be manually fixed, Amrit Williams, chief technology officer at security management solutions vendor BigFix told SCMagazineUS.com on Thursday. The worst-case scenario is that affected organizations will have to re-image each affected PC or reinstall the Windows operating system, which could take up to a full day to get the machine back up and running normally. SC Magazine

Full Story :

http://www.scmagazineus.com/mcafee-error-wreaks-havoc-on-corporate-systems/article/168557/?utm_source=feedb

• Microsoft to fix IE8 cross-site scripting problem, again

(Credit: Microsoft)

Microsoft will plug a hole in a built-in filter in Internet Explorer 8 that can be used to launch the very types of attacks on Web sites it was designed to help prevent, the company said on Tuesday.

The company will update the IE cross-site scripting (XSS) filter in June to fix a hole that researchers warned about at the Black Hat Europe conference in Barcelona last week. The researchers showed how problems with the filter could be used to inject malicious code onto sites including Google, Microsoft's Bing search site, and Twitter. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20002976-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• New Zeus version targeting Firefox users for bank fraud

A new version of the data-stealing trojan Zeus is for the first time able to successfully exploit Mozilla's Firefox browser to commit sophisticated online banking fraud, according to security firm Trusteer. Zeus, the most prevalent type of financial malware on the internet today, is known for stealing bank account information from its victims. But, previous versions of the malware were unable to bypass the security defenses, such as strong layers of authentication, used by banks when a user was on Mozilla's browser, Mickey Boodaei, CEO of Trusteer told SCMagazineUS.com on Wednesday. The newest Zeus incarnation targets Firefox browsers with techniques called HTML injection and transaction tampering, which can effectively bypass strong authentication and transaction signing.

"We expect this new version of Zeus to significantly increase fraud losses, since nearly 30 percent of internet users bank online with Firefox and the infection rate for this piece of malware is growing faster than we have ever seen before," Amit Klein, CTO of Trusteer and head of the company's research organization, said in a statement. SC Magazine

Full Story :

http://www.scmagazineus.com/new-zeus-version-targeting-firefox-users-for-bank-fraud/article/168455/?utm_source=

New Vulnerabilities Tested in SecureScout

• 18771 Windows Kernel Null Pointer Vulnerability (MS10-021/979683) (Remote File Checking)

A denial of service vulnerability exists in the Windows kernel due to the insufficient validation of registry keys passed to a Windows kernel system call. An attacker could exploit the vulnerability by running a specially crafted application, causing the system to become unresponsive and automatically restart.

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

References:

* SECTRACK: 1023850

<http://securitytracker.com/alerts/2010/Apr/1023850.html>

* VUPEN: VUPEN/ADV-2010-0865

<http://www.vupen.com/english/advisories/2010/0865>

* BID: 39297

<http://www.securityfocus.com/bid/39297>

* MS: MS10-021

<http://www.microsoft.com/technet/security/Bulletin/MS10-021.msp>

* CERT: TA10-103A

<http://www.us-cert.gov/cas/techalerts/TA10-103A.html>

CVE Reference:

CVE-2010-0234 (cve.mitre.org, nvd.nist.gov)

• 18772 Windows Kernel Symbolic Link Value Vulnerability (MS10-021/979683) (Remote File Checking)

A denial of service vulnerability exists in the Windows kernel due to the manner in which the kernel processes the values of symbolic links. An attacker could exploit the vulnerability by running a specially crafted application causing the system to become unresponsive and automatically restart.

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

References:

- * SECTRACK: 1023850
<http://securitytracker.com/alerts/2010/Apr/1023850.html>
- * VUPEN: VUPEN/ADV-2010-0865
<http://www.vupen.com/english/advisories/2010/0865>
- * BID: 39309
<http://www.securityfocus.com/bid/39309>
- * MS: MS10-021
<http://www.microsoft.com/technet/security/Bulletin/MS10-021.msp>
- * CERT: TA10-103A
<http://www.us-cert.gov/cas/techalerts/TA10-103A.html>

CVE Reference:

CVE-2010-0235 (cve.mitre.org, nvd.nist.gov)

• 18773 Windows Kernel Memory Allocation Vulnerability (MS10-021/979683) (Remote File Checking)

An elevation of privilege vulnerability exists in the Windows kernel due to the manner in which memory is allocated when extracting a symbolic link from a registry key. 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 / Gain Root** Risk: **Medium**

References:

- * SECTRACK: 1023850
<http://securitytracker.com/alerts/2010/Apr/1023850.html>
- * VUPEN: VUPEN/ADV-2010-0865
<http://www.vupen.com/english/advisories/2010/0865>
- * BID: 39323
<http://www.securityfocus.com/bid/39323>
- * MS: MS10-021
<http://www.microsoft.com/technet/security/Bulletin/MS10-021.msp>
- * CERT: TA10-103A
<http://www.us-cert.gov/cas/techalerts/TA10-103A.html>

CVE Reference:

CVE-2010-0236 (cve.mitre.org, nvd.nist.gov)

• 18774 Windows Kernel Symbolic Link Creation Vulnerability (MS10-021/979683) (Remote File Checking)

An elevation of privilege vulnerability exists when the Windows kernel does not properly restrict symbolic link creation between untrusted and trusted registry hives. 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 / Gain Root** Risk: **Medium**

References:

- * SECTRACK: 1023850
<http://securitytracker.com/alerts/2010/Apr/1023850.html>
- * VUPEN: VUPEN/ADV-2010-0865
<http://www.vupen.com/english/advisories/2010/0865>
- * BID: 39324
<http://www.securityfocus.com/bid/39324>

* MS: MS10-021

<http://www.microsoft.com/technet/security/Bulletin/MS10-021.msp>

* CERT: TA10-103A

<http://www.us-cert.gov/cas/techalerts/TA10-103A.html>

CVE Reference:

CVE-2010-0237 (cve.mitre.org, nvd.nist.gov)

• **18775 Windows Kernel Registry Key Vulnerability (MS10-021/979683) (Remote File Checking)**

A denial of service vulnerability exists in the way that the Windows kernel validates registry keys. An attacker could exploit the vulnerability by running a specially crafted application causing the system to become unresponsive and automatically restart.

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

References:

* SECTRACK: 1023850

<http://securitytracker.com/alerts/2010/Apr/1023850.html>

* VUPEN: VUPEN/ADV-2010-0865

<http://www.vupen.com/english/advisories/2010/0865>

* BID: 39318

<http://www.securityfocus.com/bid/39318>

* MS: MS10-021

<http://www.microsoft.com/technet/security/Bulletin/MS10-021.msp>

* CERT: TA10-103A

<http://www.us-cert.gov/cas/techalerts/TA10-103A.html>

CVE Reference:

CVE-2010-0238 (cve.mitre.org, nvd.nist.gov)

• **18776 Windows Virtual Path Parsing Vulnerability (MS10-021/979683) (Remote File Checking)**

A denial of service vulnerability exists in the Windows kernel due to the way that the kernel resolves the real path for a registry key from its virtual path. An attacker could exploit the vulnerability by running a specially crafted application, causing the system to become unresponsive and automatically restart.

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

References:

* SECTRACK: 1023850

<http://securitytracker.com/alerts/2010/Apr/1023850.html>

* VUPEN: VUPEN/ADV-2010-0865

<http://www.vupen.com/english/advisories/2010/0865>

* BID: 39319

<http://www.securityfocus.com/bid/39319>

* MS: MS10-021

<http://www.microsoft.com/technet/security/Bulletin/MS10-021.msp>

* CERT: TA10-103A

<http://www.us-cert.gov/cas/techalerts/TA10-103A.html>

CVE Reference:

CVE-2010-0481 (cve.mitre.org, nvd.nist.gov)

• **18777 Windows Kernel Malformed Image Vulnerability (MS10-021/979683) (Remote File Checking)**

A denial of service vulnerability exists in the Windows kernel due to the improper validation of specially crafted image files. An attacker could exploit the vulnerability by running a specially crafted application causing the system to become unresponsive and automatically restart.

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

References:

* SECTRACK: 1023850

<http://securitytracker.com/alerts/2010/Apr/1023850.html>

* VUPEN: VUPEN/ADV-2010-0865

<http://www.vupen.com/english/advisories/2010/0865>

* BID: 39320

<http://www.securityfocus.com/bid/39320>

* MS: MS10-021

<http://www.microsoft.com/technet/security/Bulletin/MS10-021.mspx>

* CERT: TA10-103A

<http://www.us-cert.gov/cas/techalerts/TA10-103A.html>

CVE Reference:

CVE-2010-0482 (cve.mitre.org, nvd.nist.gov)

• 18778 Windows Kernel Exception Handler Vulnerability (MS10-021/979683) (Remote File Checking)

A denial of service vulnerability exists in the Windows kernel due to the way that the kernel handles certain exceptions. An attacker could exploit the vulnerability by running a specially crafted application, causing the system to become unresponsive and automatically restart.

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

References:

* SECTRACK: 1023850

<http://securitytracker.com/alerts/2010/Apr/1023850.html>

* VUPEN: VUPEN/ADV-2010-0865

<http://www.vupen.com/english/advisories/2010/0865>

* BID: 39322

<http://www.securityfocus.com/bid/39322>

* MS: MS10-021

<http://www.microsoft.com/technet/security/Bulletin/MS10-021.mspx>

* CERT: TA10-103A

<http://www.us-cert.gov/cas/techalerts/TA10-103A.html>

CVE Reference:

CVE-2010-0810 (cve.mitre.org, nvd.nist.gov)

• 18779 Media Player Remote Code Execution Vulnerability (MS10-027/979402) (Remote File Checking)

A remote code execution vulnerability exists in the Windows Media Player ActiveX control. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs or view, change, or delete data with full user rights.

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

References:

* SECTRACK: 1023849

<http://securitytracker.com/alerts/2010/Apr/1023849.html>

* VUPEN: VUPEN/ADV-2010-0870

<http://www.vupen.com/english/advisories/2010/0870>

* BID: 39351

<http://www.securityfocus.com/bid/39351>

* MS: MS10-027

<http://www.microsoft.com/technet/security/Bulletin/MS10-027.mspx>

* CERT: TA10-103A

<http://www.us-cert.gov/cas/techalerts/TA10-103A.html>

CVE Reference:

CVE-2010-0268 (cve.mitre.org, nvd.nist.gov)

• 18780 Media Services Stack-based Buffer Overflow Vulnerability (MS10-025/980858) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Windows 2000 Server Service Pack 4 running the optional Windows Media Services component due to the way the Windows Media Unicast Service handles specially crafted transport information packets. On Microsoft Windows 2000 Server Service Pack 4, Windows Media Services is an optional component and is not installed by default. Only Microsoft Windows 2000 Server systems that have enabled Windows Media Services are affected by this vulnerability.

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

References:

* SECTRACK: 1023851

<http://securitytracker.com/alerts/2010/Apr/1023851.html>

* VUPEN: VUPEN/ADV-2010-0868

<http://www.vupen.com/english/advisories/2010/0868>

* MS: MS10-025

<http://www.microsoft.com/technet/security/Bulletin/MS10-025.mspx>

* CERT: TA10-103A

<http://www.us-cert.gov/cas/techalerts/TA10-103A.html>

CVE Reference:

CVE-2010-0478 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-1489 Microsoft CVSS 2.0 Score = 4.3

The XSS Filter in Microsoft Internet Explorer 8 does not properly perform neutering for the SCRIPT tag, which allows remote attackers to conduct cross-site scripting (XSS) attacks against web sites that have no inherent XSS vulnerabilities, a different issue than CVE-2009-4074.

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

References:

MISC: http://p42.us/ie8xss/Abusing_IE8s_XSS_Filters.pdf

MISC: <http://p42.us/ie8xss/>

CONFIRM: <http://blogs.technet.com/msrc/archive/2010/04/19/guidance-on-internet-explorer-xss-filter.aspx>

CVE Reference: [CVE-2010-1489](http://cve.mitre.org/cve/2010/1489)

• CVE-2010-1151 Apache CVSS 2.0 Score = 6.8

Race condition in the mod_auth_shadow module for the Apache HTTP Server allows remote attackers to bypass authentication, and read and possibly modify data, via vectors related to improper interaction with an external helper application for validation of credentials.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=578168

VUPEN: <http://www.vupen.com/english/advisories/2010/0908>

MANDRIVA: <http://www.mandriva.com/security/advisories?name=MDVSA-2010:081>

CVE Reference: [CVE-2010-1151](http://cve.mitre.org/cve/2010/1151)

• CVE-2010-1033 HP CVSS 2.0 Score = 9.3

Multiple stack-based buffer overflows in a certain Tetrydyne ActiveX control in HP Operations Manager 7.5, 8.10, and 8.16 might allow remote attackers to execute arbitrary code via a long string argument to the (1) LoadFile or (2) SaveFile method, related to srcvw32.dll and srcvw4.dll.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/57938>

VUPEN: <http://www.vupen.com/english/advisories/2010/0946>

BID: <http://www.securityfocus.com/bid/39578>

MISC: http://www.corelan.be:8800/wp-content/forum-file-uploads/mr_me/hpoperationsmng.html.txt

MISC: <http://www.corelan.be:8800/advisories.php?id=CORELAN-10-027>

SECTRACK: <http://securitytracker.com/id?1023894>

SECUNIA: <http://secunia.com/advisories/39538>

MISC: <http://net-ninja.net/blog/media/blogs/b/exploits/hpoperationsmngr.html.txt>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02078800>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02078800>

CVE Reference: [CVE-2010-1033](#)

• **CVE-2010-1032 HP CVSS 2.0 Score = 4.9**

Unspecified vulnerability in HP HP-UX B.11.11 allows local users to cause a denial of service via unknown vectors.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/0948>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02091749>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02091749>

CVE Reference: [CVE-2010-1032](#)

• **CVE-2010-1487 IBM CVSS 2.0 Score = 7.2**

IBM Lotus Notes 7.0, 8.0, and 8.5 stores administrative credentials in cleartext in SURunAs.exe, which allows local users to obtain sensitive information by examining this file, aka SPR JSTN837SEG.

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

References:

BID: <http://www.securityfocus.com/bid/39525>

SECUNIA: <http://secunia.com/advisories/39507>

CVE Reference: [CVE-2010-1487](#)

• **CVE-2010-0593 Cisco CVSS 2.0 Score = 9.0**

The Cisco RVS4000 4-port Gigabit Security Router before 1.3.2.0, PVC2300 Business Internet Video Camera before 1.1.2.6, WVC200 Wireless-G PTZ Internet Video Camera before 1.1.1.15, WVC210 Wireless-G PTZ Internet Video Camera before 1.1.1.15, and WVC2300 Wireless-G Business Internet Video Camera before 1.1.2.6 do not properly restrict read access to passwords, which allows context-dependent attackers to obtain sensitive information, related to (1) access by remote authenticated users to a PVC2300 or WVC2300 via a crafted URL, (2) leveraging setup privileges on a WVC200 or WVC210, and (3) leveraging administrative privileges on an RVS4000, aka Bug ID CSCte64726.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b27511.shtml

CVE Reference: [CVE-2010-0593](#)

• **CVE-2010-1318 RealNetworks CVSS 2.0 Score = 10.0**

Stack-based buffer overflow in the AgentX::receive_agentx function in AgentX++ 1.4.16, as used in RealNetworks Helix Server and Helix Mobile Server 11.x through 13.x and other products, allows remote attackers to execute arbitrary code via unspecified vectors.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/0889>

BID: <http://www.securityfocus.com/bid/39490>

CONFIRM: <http://www.realnetworks.com/uploadedFiles/Support/helix-support/SecurityUpdate041410HS.pdf>

SECUNIA: <http://secunia.com/advisories/39279>

CVE Reference: [CVE-2010-1318](#)

• **CVE-2010-1319 RealNetworks CVSS 2.0 Score = 10.0**

Integer overflow in the AgentX::receive_agentx function in AgentX++ 1.4.16, as used in RealNetworks Helix Server and Helix Mobile Server 11.x through 13.x and other products, allows remote attackers to execute arbitrary code via a request with a crafted payload length.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/0889>

BID: <http://www.securityfocus.com/bid/39490>

CONFIRM: <http://www.realnetworks.com/uploadedFiles/Support/helix-support/SecurityUpdate041410HS.pdf>

SECUNIA: <http://secunia.com/advisories/39279>

CVE Reference: [CVE-2010-1319](#)

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