

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://www2.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

[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://www2.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

This Week in Review

Trojan spreading via 0-day vulnerability. Wordpress sites under attack. ISP's seen as most able to protect against botnets. Anonymous fighting drug cartel.

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

• Duqu trojan spreads through 0-day Microsoft bug

Duqu, the so-called "son of Stuxnet" trojan, contains a dropper program that exploits a previously unknown vulnerability in the Windows kernel, researchers said Tuesday.

This adds merit to security industry suspicions that Duqu is a sophisticated piece of malware, possibly containing underlying Stuxnet code. Analysts have suggested that Duqu was created to conduct reconnaissance of target industrial control systems, and may be a precursor to another Stuxnet-like attack.

The zero-day exploit was confirmed by the Laboratory of Cryptography and System Security (CrySyS), a Budapest, Hungary-based facility that originally discovered Duqu. SC Magazine

Full Story :

http://www.scmagazineus.com/duqu-trojan-spreads-through-0-day-microsoft-bug/article/215797/?utm_source=feed

• **Thousands of WordPress sites sucked into BlackHole**

Researchers have discovered a spike in malware infecting thousands of WordPress websites that use a popular image tool.

The attacks came to light after French media outlet, The Poitou-Charentes Journal, began hosting on malicious code on its WordPress site.

Avast senior researcher Jan Sirmer found attackers had exploited weak FTP server authentication credentials and a vulnerability in the TimThumb image resizer to upload malicious PHP files to the site. SC Magazine

Full Story :

http://www.scmagazineus.com/thousands-of-wordpress-sites-sucked-into-blackhole/article/215808/?utm_source=feed

• **Feedback due on gov't proposal around botnet notification**

Many view internet service providers (ISPs) as the entity with the most ability to do something about the botnet scourge. That's why the U.S. Commerce and Homeland Security departments are seeking feedback on a program that would build incentive-driven codes of conduct for ISPs to voluntarily detect, notify and possibly assist in the removal of malware on consumers' machines.

Public comments are due by Friday.

"In our country, we always have this debate whether the government should take a stronger hand or whether market forces are enough," Cameron Kerry, general counsel at the U.S. Department of Commerce, said during a recent discussion on the topic, organized by the Center for Strategic and International Studies (CSIS). "We've run out of time to have that conversation, at least on some level. We have to get something done." SC Magazine

Full Story :

http://www.scmagazineus.com/feedback-due-on-govt-proposal-around-botnet-notification/article/215778/?utm_source=feed

• **Anonymous ready to continue with Operation Cartel**

A plan by hactivist group Anonymous to expose the details of people connected to one of the world's most dangerous drug cartels is back on after being briefly canceled, according to a video posted Wednesday by Barrett Brown, who regularly communicates with the hacker collective.

"This was canceled earlier this morning by one of the people involved," said Brown, a former spokesman for Anonymous. "Shortly thereafter, the assembled people held a vote and decided nonetheless to go ahead with the operation."

Brown's video shed some light on the nature of the risky undertaking, dubbed Operation Cartel, or OpCartel, which was hatched last month as a means to avenge the kidnapping of an Anonymous member by the powerful Zetas drug cartel. The Anonymous member reportedly was abducted in the eastern Mexican state of Veracruz while participating in an anti-cartel march. SC Magazine

Full Story :

http://www.scmagazineus.com/anonymous-ready-to-continue-with-operation-cartel/article/215883/?utm_source=feed

New Vulnerabilities Tested in SecureScout

• **19553 Microsoft Internet Explorer Uninitialized Object Memory Corruption Vulnerability (MS11-081/2586448) (Remote File Checking)**

Microsoft Internet Explorer is prone to a remote memory-corruption vulnerability.

Microsoft Internet Explorer 6 through 9 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing a deleted object, aka "Scroll Event Remote Code Execution Vulnerability."

Successful exploits will allow an attacker to run arbitrary code in the context of the user running the application. Failed attacks may cause denial-of-service conditions.

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

References:

- * MS: MS11-081
<http://technet.microsoft.com/en-us/security/bulletin/MS11-081>
- * BID: 49947
<http://www.securityfocus.com/bid/49947>

CVE Reference:

CVE-2011-1993 (cve.mitre.org, nvd.nist.gov)

• 19554 Microsoft Internet Explorer 'OLEAuto32.dll' Memory Corruption Vulnerability (MS11-081/2586448) (Remote File Checking)

Microsoft Internet Explorer is prone to a remote memory-corruption vulnerability.

Microsoft Internet Explorer 6 through 9 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that was not properly initialized, aka "OLEAuto32.dll Remote Code Execution Vulnerability."

Successful exploits will allow an attacker to run arbitrary code in the context of the user running the application. Failed attacks may cause denial-of-service condition

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

References:

- * BID: 49960
<http://www.securityfocus.com/bid/49960>
- * MS: MS11-081
<http://technet.microsoft.com/en-us/security/bulletin/MS11-081>

CVE Reference:

CVE-2011-1995 (cve.mitre.org, nvd.nist.gov)

• 19555 Microsoft Internet Explorer Option Element Memory Corruption Vulnerability (MS11-081/2586448) (Remote File Checking)

Microsoft Internet Explorer is prone to a remote memory-corruption vulnerability.

Microsoft Internet Explorer 6 through 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing a deleted object, aka "Option Element Remote Code Execution Vulnerability."

Successful exploits will allow an attacker to run arbitrary code in the context of the user running the application. Failed attacks may cause denial-of-service conditions.

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

References:

- * MS: MS11-081
<http://technet.microsoft.com/en-us/security/bulletin/MS11-081>
- * MISC: Ivan Fratric's Security Blog
<http://ifsec.blogspot.com/2011/10/internet-explorer-option-element-remote.html>
- * BID: 49961
<http://www.securityfocus.com/bid/49961/info>

CVE Reference:

CVE-2011-1996 (cve.mitre.org, nvd.nist.gov)

• 19556 Microsoft Internet Explorer OnLoad Event Memory Corruption Vulnerability (MS11-081/2586448) (Remote File Checking)

Microsoft Internet Explorer is prone to a remote memory-corruption vulnerability.

Microsoft Internet Explorer 6 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing a deleted object, aka "OnLoad Event Remote Code Execution Vulnerability."

Successful exploits will allow an attacker to run arbitrary code in the context of the user running the application. Failed attacks may cause denial-of-service conditions.

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

References:

- * BID: 49962
<http://www.securityfocus.com/bid/49962>
- * MS: MS11-081
<http://technet.microsoft.com/en-us/security/bulletin/MS11-081>

CVE Reference:

CVE-2011-1997 (cve.mitre.org, nvd.nist.gov)

• 19557 Microsoft Internet Explorer 'Jscript9.dll' Memory Corruption Vulnerability (MS11-081/2586448) (Remote File Checking)

Microsoft Internet Explorer is prone to a remote memory-corruption vulnerability.

Microsoft Internet Explorer 9 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that was not properly initialized, aka "Jscript9.dll Remote Code Execution Vulnerability."

Successful exploits will allow an attacker to run arbitrary code in the context of the user running the application. Failed attacks may cause denial-of-service conditions.

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

References:

- * MS: MS11-081
<http://technet.microsoft.com/en-us/security/bulletin/MS11-081>
- * BID: 49963
<http://www.securityfocus.com/bid/49963/info>
- * MISC: Avaya System Products:
<http://support.avaya.com/css/P8/documents/100149804>

CVE Reference:

CVE-2011-1998 (cve.mitre.org, nvd.nist.gov)

• 19558 Microsoft Internet Explorer Select Element Memory Corruption Vulnerability (MS11-081/2586448) (Remote File Checking)

Microsoft Internet Explorer is prone to a remote memory-corruption vulnerability.

Microsoft Internet Explorer 8 does not properly allocate and access memory, which allows remote attackers to execute arbitrary code via vectors involving a "dereferenced memory address," aka "Select Element Remote Code Execution Vulnerability."

Successful exploits will allow an attacker to run arbitrary code in the context of the user running the application. Failed attacks may cause denial-of-service conditions.

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

References:

- * BID: 49964
<http://www.securityfocus.com/bid/49964/info>
- * MS: MS11-081
<http://technet.microsoft.com/en-us/security/bulletin/MS11-081>
- * MISC: Ivan Fratric's Security Blog
<http://ifsec.blogspot.com/2011/10/internet-explorer-select-element-remote.html>

CVE Reference:

CVE-2011-1999 (cve.mitre.org, nvd.nist.gov)

• 19559 Microsoft Internet Explorer 'SwapNode()' Memory Corruption Vulnerability (MS11-081/2586448) (Remote File Checking)

Microsoft Internet Explorer is prone to a remote memory-corruption vulnerability.

Microsoft Internet Explorer 6 through 9 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing a deleted object, aka "Body Element Remote Code Execution Vulnerability."

Successful exploits will allow an attacker to run arbitrary code in the context of the user running the application. Failed attacks may cause denial-of-service conditions.

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

References:

- * BID: 49965
<http://www.securityfocus.com/bid/49965/info>
- * MS: MS11-081
<http://technet.microsoft.com/en-us/security/bulletin/MS11-081>
- * MISC: Avaya System Products:
<http://support.avaya.com/css/P8/documents/100149804>

CVE Reference:

CVE-2011-2000 (cve.mitre.org, nvd.nist.gov)

• **19560 Microsoft Internet Explorer Virtual Function Table Memory Corruption Vulnerability (MS11-081/2586448) (Remote File Checking)**

Microsoft Internet Explorer is prone to a remote memory-corruption vulnerability.

Microsoft Internet Explorer 6 through 9 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code via an attempted access to a virtual function table after corruption of this table has occurred, aka "Virtual Function Table Corruption Remote Code Execution Vulnerability."

Successful exploits will allow an attacker to run arbitrary code in the context of the user running the application. Failed attacks may cause denial-of-service conditions.

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

References:

- * BID: 49966
<http://www.securityfocus.com/bid/49966/info>
- * MS: MS11-081
<http://technet.microsoft.com/en-us/security/bulletin/MS11-081>
- * MISC: TippingPoint Zero Day Initiative
[http://www.zerodayinitiative.com/advisories/ZDI-11-290/?utm_source=feedburner&utm_medium=feed&utm_campaign=ZDI-Published-Advisories%28Zero Day Initiative Published Advisories%29](http://www.zerodayinitiative.com/advisories/ZDI-11-290/?utm_source=feedburner&utm_medium=feed&utm_campaign=ZDI-Published-Advisories%28Zero%20Day%20Initiative%20Published%20Advisories%29)
- * MISC: Avaya System Products:
<http://support.avaya.com/css/P8/documents/100149804>

CVE Reference:

CVE-2011-2001 (cve.mitre.org, nvd.nist.gov)

• **19563 Apple QuickTime Movie File Handling Integer Overflow Vulnerability**

Apple QuickTime is prone to an integer-overflow vulnerability due to a failure to properly bounds-check user-supplied data.

Integer overflow in Apple QuickTime before 7.7.1 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted movie file with JPEG2000 encoding. The problem occurs when handling a specially crafted movie file. Successful exploits may allow attackers to execute arbitrary code in the context of the currently logged-in user; failed exploit attempts may cause denial-of-service conditions.

Versions prior to QuickTime 7.7.1 are vulnerable on Windows 7, Vista, and XP.

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

References:

- * CONFIRM:
<http://support.apple.com/kb/HT5016>
- * BID: 50401
<http://www.securityfocus.com/bid/50401/info>
- * MISC:
<http://www.security-database.com/detail.php?alert=CVE-2011-3250>

CVE Reference:

CVE-2011-3250 (cve.mitre.org, nvd.nist.gov)

• **19564 Apple QuickTime TKHD Atoms Handling Remote Code Execution Vulnerability**

Apple QuickTime before 7.7.1 on Windows is prone to a remote code-execution vulnerability due to a failure of handling TKHD atoms in QuickTime movie files. It may allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via crafted TKHD atoms in a QuickTime movie file.

The problem occurs when handling a specially crafted movie file. Successful exploits may allow attackers to execute arbitrary code in the context of the currently logged-in user; failed exploit attempts may cause denial-of-service conditions.

Versions prior to QuickTime 7.7.1 are vulnerable on Windows 7, Vista, and XP.

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

References:

* BID: 50403

<http://www.securityfocus.com/bid/50403/info>

* MISC:

<http://www.security-database.com/detail.php?alert=CVE-2011-3251>

* CONFIRM:

<http://support.apple.com/kb/HT5016>

CVE Reference:

CVE-2011-3251 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-3167 HP CVSS 2.0 Score = 6.4

Unspecified vulnerability in HP OpenView Network Node Manager (OV NNM) 7.51 and 7.53 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-1210.

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

References:

HP: <http://marc.info/?l=bugtraq&m=132017799623289&w=2>

HP: <http://marc.info/?l=bugtraq&m=132017799623289&w=2>

CVE Reference: [CVE-2011-3167](http://cve.mitre.org/cve/2011/3167)

• CVE-2011-3165 HP CVSS 2.0 Score = 6.4

Unspecified vulnerability in HP OpenView Network Node Manager (OV NNM) 7.51 and 7.53 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-1208.

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

References:

HP: <http://marc.info/?l=bugtraq&m=132017799623289&w=2>

HP: <http://marc.info/?l=bugtraq&m=132017799623289&w=2>

CVE Reference: [CVE-2011-3165](http://cve.mitre.org/cve/2011/3165)

• CVE-2011-3166 HP CVSS 2.0 Score = 6.4

Unspecified vulnerability in HP OpenView Network Node Manager (OV NNM) 7.51 and 7.53 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-1209.

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

References:

HP: <http://marc.info/?l=bugtraq&m=132017799623289&w=2>

HP: <http://marc.info/?l=bugtraq&m=132017799623289&w=2>

CVE Reference: [CVE-2011-3166](http://cve.mitre.org/cve/2011/3166)

• CVE-2011-1367 IBM CVSS 2.0 Score = 9.3

Unspecified vulnerability in the File Load feature in IBM Rational AppScan Standard and Express 7.8.x, 7.9.x, and 8.0.x before 8.0.0.3 allows remote attackers to execute arbitrary commands via a crafted .scan file.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/70044>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21515110>

CVE Reference: [CVE-2011-1367](#)

• **CVE-2011-1366 IBM CVSS 2.0 Score = 8.8**

Unspecified vulnerability in the Import feature in IBM Rational AppScan Enterprise and AppScan Reporting Console 5.2 through 7.9.x and 8.x before 8.0.1.1 allows remote attackers to execute arbitrary commands on an agent server via a crafted ZIP archive.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/70043>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21515110>

CVE Reference: [CVE-2011-1366](#)

• **CVE-2011-1368 IBM CVSS 2.0 Score = 5.0**

The JavaServer Faces (JSF) application functionality in IBM WebSphere Application Server 8.x before 8.0.0.1 does not properly handle requests, which allows remote attackers to read unspecified files via unknown vectors.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/70168>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=swg1PM45992>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg24030916>

CVE Reference: [CVE-2011-1368](#)

• **CVE-2011-4005 Cisco CVSS 2.0 Score = 9.3**

Cross-site request forgery (CSRF) vulnerability in the Services Ready Platform Configuration Utility web interface on the Cisco Small Business SRP521W, SRP526W, and SRP527W with firmware before 1.1.24 and the Small Business SRP541W, SRP546W, and SRP547W with firmware before 1.2.1 allows remote attackers to hijack the authentication of administrators for requests that execute arbitrary commands, aka Bug ID CSCtr45124.

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

References:

CISCO: <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111102-srp500>

CVE Reference: [CVE-2011-4005](#)

• **CVE-2011-0941 Cisco CVSS 2.0 Score = 7.8**

Memory leak in Cisco Unified Communications Manager (CUCM) 6.x before 6.1(5)su2, 7.x before 7.1(5b)su3, 8.x before 8.0(3a)su1, and 8.5 before 8.5(1) allows remote attackers to cause a denial of service (memory consumption and process failure) via a malformed SIP message, aka Bug ID CSCti75128.

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

References:

CISCO: <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-cucm>

CVE Reference: [CVE-2011-0941](#)

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