

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>

This Week in Review

LulzSec taking down CIA. Virtualization guidelines from PCI council. Scam via the phone. Chinese react to US cyber war talk.

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

• CIA Web site down; LulzSec claims responsibility

(Credit: Screen capture by Eric Mack/CNET) The CIA's public Web site is inaccessible this afternoon, and the hacking group Lulz Security is taking for responsibility for taking it offline.

Shortly before 3 p.m. PT, LulzSec tweeted: "Tango down - cia.gov - for the lulz"

And indeed, the world's most famous spy agency is currently without an official Web presence, as of about 20 minutes after Lulzsec's tweet--cia.gov returns an error message. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20071387-83/cia-web-site-down-lulzsec-claims-responsibility/?part=rss&subj=new

• Virtualization guidelines issued to supplement PCI DSS 2.0

The PCI Security Standards Council, an organization comprised of the leading credit card brands and with a mission to thwart data leakage and stop payment cardholder data fraud, on Tuesday released "PCI DSS Virtualization Guidelines."

The 39-page document provides guidance to those enterprises in the payment chain on the use of virtualization technology in relation to their compliance with the Payment Card Industry Data Security Standard (PCI DSS).

The guidance helps to update PCI DSS into the era of cloud computing, a demand strongly urged after the last PCI DSS update in August failed to address such hot-button items as tokenization, chip-and PIN and end-to-end encryption. SC Magazine

Full Story :

http://www.scmagazineus.com/virtualization-guidelines-issued-to-supplement-pci-dss-20/article/205274/?utm_source=

• Scammers turning to phone calls to gain PC access

Forget e-mail. Criminals are making old-fashioned phone calls and offering free security scans in order to gain access to people's computers, according to Microsoft.

To run the con, criminals pretend to be PC security experts from legitimate companies. They call their intended victims, warning of a risky security threat and offering to run a free security checkup. If the victims take the bait, the scammers gain access to their PCs and often capture passwords or financial information.

The phone is a tried and true method for cons. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20071568-83/scammers-turning-to-phone-calls-to-gain-pc-access/?part=rss&subj=

• Chinese military warns of U.S. cyberwar threat

The Chinese military wants to beef up its cyberdefense efforts as it anticipates greater threats originating from the U.S.

"The U.S. military is hastening to seize the commanding military heights on the Internet, and another Internet war is being pushed to a stormy peak," the Chinese military wrote in its official newspaper, Liberation Army Daily. "Their actions remind us that to protect the nation's Internet security, we must accelerate Internet defense development and accelerate steps to make a strong Internet army."

Though Liberation Army Daily isn't an official mouthpiece for the Chinese government, Reuters, which first reported on the story, points out that it typically reflects the official opinion of China's ruling party. Cnet Security

Full Story :

http://news.cnet.com/8301-13506_3-20071553-17/chinese-military-warns-of-u.s-cyberwar-threat/?part=rss&subj=news=

New Vulnerabilities Tested in SecureScout

• 19368 Yamaha routers IP header options Denial of Service Vulnerability

Yamaha RTX, RT, SRT, RTV, RTW, and RTA series routers with firmware 6.x through 10.x, and NEC IP38X series routers with firmware 6.x through 10.x, do not properly handle IP header options, which allows remote attackers to cause a denial of service (device reboot) via a crafted option that triggers access to an invalid memory location.

The firmware versions that address the issues are:

RTX3000 Since Rev.9.00.48
RTX2000 Since Rev.7.01.55
RTX1500 Since Rev.8.03.87
RTX1200 Since Rev.10.01.22
RTX1100 Since Rev.8.03.87
RTX1000 Since Rev.7.01.55, Since Rev.8.01.29
SRT100 Since Rev.10.00.52
RTV700 Since Rev.8.00.94
RT300i Since Rev.6.03.39
RT250i Since Rev.8.02.51
RT107e Since Rev.8.03.87
RT58i Since Rev.9.01.48
RT57i Since Rev.8.00.95

The following routers have no firmware updates that address the issue and thus remain vulnerable:

RT105 Series
RT56v

RTW65i, RTW65b, RT60w
RTA55i, RTA54i, RTA52i, RTA50i
RT140 Series
RT200i, RT103i, RT102i, RT100i, RT80i

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

References:

- * CONFIRM:
<http://www.nec.co.jp/security-info/secinfo/nv11-004.html>
- * CONFIRM:
<http://www.rpro.yamaha.co.jp/RT/FAQ/Security/JVN55714408.html>
- * JVN: JVN#55714408
<http://jvn.jp/en/jp/JVN55714408/index.html>
- * BID: 47294
<http://www.securityfocus.com/bid/47294>

CVE Reference:

CVE-2011-1323 (cve.mitre.org, nvd.nist.gov)

• **19369 MIME Sniffing Information Disclosure Vulnerability (MS11-050/2530548) (Remote File Checking)**

An information disclosure vulnerability exists in Internet Explorer that could allow an attacker to force the browser to perform unexpected actions when a user downloads Web content, allowing an attacker to view content from a different domain or Internet Explorer zone other than the domain or zone of the attacker's Web page.

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

References:

- * MS: MS11-050
<http://www.microsoft.com/technet/security/Bulletin/MS11-050.mspx>
- * BID: 48200
<http://www.securityfocus.com/bid/48200>
- * SECTRACK: 1025649
<http://securitytracker.com/id/1025649>

CVE Reference:

CVE-2011-1246 (cve.mitre.org, nvd.nist.gov)

• **19370 Link Properties Handling Memory Corruption Vulnerability (MS11-050/2530548) (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. The vulnerability may corrupt memory in such a way that an attacker could execute arbitrary code in the context of the logged-on user.

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

References:

- * MS: MS11-050
<http://www.microsoft.com/technet/security/Bulletin/MS11-050.mspx>
- * BID: 48202
<http://www.securityfocus.com/bid/48202>
- * SECTRACK: 1025649
<http://securitytracker.com/id/1025649>

CVE Reference:

CVE-2011-1250 (cve.mitre.org, nvd.nist.gov)

• **19371 DOM Manipulation Memory Corruption Vulnerability (MS11-050/2530548) (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. The vulnerability may corrupt memory in such a way that an attacker could execute arbitrary code in the context of the logged-on user.

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

References:

* MS: MS11-050

<http://www.microsoft.com/technet/security/Bulletin/MS11-050.mspx>

* BID: 48203

<http://www.securityfocus.com/bid/48203>

* SECTRACK: 1025649

<http://securitytracker.com/id/1025649>

CVE Reference:

CVE-2011-1251 (cve.mitre.org, nvd.nist.gov)

• **19372 toStaticHTML Information Disclosure Vulnerability (MS11-050/2530548) (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: **Gather Info** Risk: **Medium**

References:

* MS: MS11-050

<http://www.microsoft.com/technet/security/Bulletin/MS11-050.mspx>

* BID: 48199

<http://www.securityfocus.com/bid/48199>

* SECTRACK: 1025649

<http://securitytracker.com/id/1025649>

CVE Reference:

CVE-2011-1252 (cve.mitre.org, nvd.nist.gov)

• **19373 Drag and Drop Memory Corruption Vulnerability (MS11-050/2530548) (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. The vulnerability may corrupt memory in such a way that an attacker could execute arbitrary code in the context of the logged-on user.

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

References:

* MS: MS11-050

<http://www.microsoft.com/technet/security/Bulletin/MS11-050.mspx>

* BID: 48204

<http://www.securityfocus.com/bid/48204>

* SECTRACK: 1025649

<http://securitytracker.com/id/1025649>

CVE Reference:

CVE-2011-1254 (cve.mitre.org, nvd.nist.gov)

• **19374 Time Element Memory Corruption Vulnerability (MS11-050/2530548) (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. The vulnerability may corrupt memory in such a way that an attacker could execute arbitrary code in the context of the logged-on user.

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

References:

* MS: MS11-050

<http://www.microsoft.com/technet/security/Bulletin/MS11-050.mspx>

* BID: 48206

<http://www.securityfocus.com/bid/48206>

* SECTRACK: 1025649

<http://securitytracker.com/id/1025649>

CVE Reference:

CVE-2011-1255 (cve.mitre.org, nvd.nist.gov)

• **19375 DOM Modification Memory Corruption Vulnerability (MS11-050/2530548) (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. The vulnerability may corrupt memory in such a way that an attacker could execute arbitrary code in the context of the logged-on user.

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

References:

- * MS: MS11-050
<http://www.microsoft.com/technet/security/Bulletin/MS11-050.msp>
- * BID: 48207
<http://www.securityfocus.com/bid/48207>
- * SECTRACK: 1025649
<http://securitytracker.com/id/1025649>

CVE Reference:

CVE-2011-1256 (cve.mitre.org, nvd.nist.gov)

• **19376 Drag and Drop Information Disclosure Vulnerability (MS11-050/2530548) (Remote File Checking)**

An information disclosure vulnerability exists in Internet Explorer that could allow script to gain access to information in another domain or Internet Explorer zone. 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 and performed a drag-and-drop operation. An attacker who successfully exploited this vulnerability could view content from another domain or Internet Explorer zone.

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

References:

- * MS: MS11-050
<http://www.microsoft.com/technet/security/Bulletin/MS11-050.msp>
- * BID: 48201
<http://www.securityfocus.com/bid/48201>
- * SECTRACK: 1025649
<http://securitytracker.com/id/1025649>

CVE Reference:

CVE-2011-1258 (cve.mitre.org, nvd.nist.gov)

• **19377 Layout Memory Corruption Vulnerability (MS11-050/2530548) (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. The vulnerability may corrupt memory in such a way that an attacker could execute arbitrary code in the context of the logged-on user.

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

References:

- * MS: MS11-050
<http://www.microsoft.com/technet/security/Bulletin/MS11-050.msp>
- * BID: 48208
<http://www.securityfocus.com/bid/48208>
- * SECTRACK: 1025649
<http://securitytracker.com/id/1025649>

CVE Reference:

CVE-2011-1260 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2011-1864** HP CVSS 2.0 Score = 9.3

Unspecified vulnerability in HP OpenView Storage Data Protector 6.0, 6.10, and 6.11 allows remote attackers to execute arbitrary code via unknown vectors.

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

References:

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02712867

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02712867

CVE Reference: [CVE-2011-1864](#)

• **CVE-2011-1861 HP CVSS 2.0 Score = 8.3**

Unspecified vulnerability in HP Service Manager 7.02, 7.11, 9.20, and 9.21 and Service Center 6.2.8 allows remote attackers to modify data or obtain sensitive information via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=130755929821099&w=2>

HP: <http://marc.info/?l=bugtraq&m=130755929821099&w=2>

CVE Reference: [CVE-2011-1861](#)

• **CVE-2011-1857 HP CVSS 2.0 Score = 8.2**

Unspecified vulnerability in HP Service Manager 7.02, 7.11, 9.20, and 9.21 and Service Center 6.2.8 allows remote authenticated users to bypass intended access restrictions via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=130755929821099&w=2>

HP: <http://marc.info/?l=bugtraq&m=130755929821099&w=2>

CVE Reference: [CVE-2011-1857](#)

• **CVE-2011-1863 HP CVSS 2.0 Score = 7.5**

HP Service Manager 7.02, 7.11, 9.20, and 9.21 and Service Center 6.2.8 allow remote authenticated users to conduct unspecified script injection attacks via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=130755929821099&w=2>

HP: <http://marc.info/?l=bugtraq&m=130755929821099&w=2>

CVE Reference: [CVE-2011-1863](#)

• **CVE-2011-1860 HP CVSS 2.0 Score = 5.0**

Unspecified vulnerability in HP Service Manager 7.02, 7.11, 9.20, and 9.21 and Service Center 6.2.8 allows remote attackers to capture HTTP session credentials via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=130755929821099&w=2>

HP: <http://marc.info/?l=bugtraq&m=130755929821099&w=2>

CVE Reference: [CVE-2011-1860](#)

• **CVE-2011-1859 HP CVSS 2.0 Score = 5.0**

Unspecified vulnerability in HP Service Manager 7.02, 7.11, 9.20, and 9.21 and Service Center 6.2.8 allows remote attackers to obtain sensitive information via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=130755929821099&w=2>

HP: <http://marc.info/?l=bugtraq&m=130755929821099&w=2>

CVE Reference: [CVE-2011-1859](#)

• **CVE-2011-1858 HP CVSS 2.0 Score = 4.3**

Unspecified vulnerability in HP Service Manager 7.02, 7.11, 9.20, and 9.21 and Service Center 6.2.8 allows local users to bypass intended access restrictions via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=130755929821099&w=2>

HP: <http://marc.info/?l=bugtraq&m=130755929821099&w=2>

CVE Reference: [CVE-2011-1858](#)

• **CVE-2011-1862 HP CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in HP Service Manager 7.02, 7.11, 9.20, and 9.21 and Service Center 6.2.8 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=130755929821099&w=2>

HP: <http://marc.info/?l=bugtraq&m=130755929821099&w=2>

CVE Reference: [CVE-2011-1862](#)

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