

2010 Issue #33

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

New PCI rules on the way. Large seller of stolen credit card numbers arrested. Heartland under attack again. Stuxnet worm could hijack power plants.

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

• Revisions to credit card security standard on the way

Network World - It will be called the Payment Card Industry Data Security Standard 2.0, and the full-blown text of this upcoming standard that governs how businesses must guard sensitive cardholder information on their networks will be out at the beginning of September, according to the organization in charge of it.

Would PCI compliance help or hurt cloud computing security?

There won't be major changes from the current DSS 1.2, according to Bob Russo, general manager of the PCI Security Standards Council. But DSS v. 2.0 will seek to clarify what the PCI requirements mean in terms of enterprise security. Computerworld

Full Story :

http://www.computerworld.com/s/article/9180603/Revisions_to_credit_card_security_standard_on_the_way?source=

• Russian charged with selling credit card numbers online

IDG News Service - A Russian man accused of selling stolen credit card numbers online for nearly a decade has been arrested in Nice, France, and faces charges in an indictment unsealed Wednesday, the U.S. Department of Justice said.

Vladislav Anatolievich Horohorin, 27, was arrested by French authorities on Saturday as he attempted to board a flight to Moscow, the DOJ said. Horohorin, who called himself BadB online, advertised himself as one of the largest sellers of stolen credit and debit cards worldwide, the DOJ said in a grand jury indictment issued in November.

Horohorin, of Moscow, said in an April 2009 advertisement of his services that he had been selling "dumps" -- compromised credit and debit card numbers -- through Web sites such as the now-closed Cardplanet.com for about eight years. Computerworld

Full Story :

http://www.computerworld.com/s/article/9180589/Russian_charged_with_selling_credit_card_numbers_online?source=...

• Heartland denies systems involved in new data breach

Computerworld - Heartland Payment Systems, which last year suffered the largest ever data breach involving payment card data, is downplaying reports out of Austin, Texas linking the payment processor to a data breach at a local restaurant chain.

Heartland CIO Steven Elefant told Computerworld by e-mail late Thursday that the reports out of Austin point to a "localized intrusion initiated within the stores, either in their point-of-sale system or as a result of other fraud."

"The Heartland system at large and its merchants would not be compromised in any way by this type of attack, and the company is unaware of any broader issue," he said. Computerworld

Full Story :

http://www.computerworld.com/s/article/9180660/Heartland_denies_systems_involved_in_new_data_breach?source=...

• Stuxnet could hijack power plants, refineries

A worm that targets critical infrastructure companies doesn't just steal data, it leaves a back door that could be used to remotely and secretly control plant operations, a Symantec researcher said on Thursday.

The Stuxnet worm infected industrial control system companies around the world, particularly in Iran and India but also companies in the U.S. energy industry, Liam O'Murchu, manager of operations for Symantec Security Response, told CNET. He declined to say how many companies may have been infected or to identify any of them.

"This is quite a serious development in the threat landscape," he said. "It's essentially giving an attacker control of the physical system in an industrial control environment." Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20013545-245.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 18873 Apache Tomcat Remote Denial Of Service and Information Disclosure Vulnerability

Apache Tomcat is a freely available, open source application server maintained by the Apache Foundation.

Several flaws in the handling of the 'Transfer-Encoding' header were found that prevented the recycling of a buffer. A remote attacker could trigger this flaw which would cause subsequent requests to fail and/or information to leak between requests. This flaw is mitigated if Tomcat is behind a reverse proxy (such as Apache httpd 2.2) as the proxy should reject the invalid transfer encoding header.

The issue has been addressed in Apache Tomcat version 6.0.26, 5.5.30.

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

References:

* BUGTRAQ: 20100709 [SECURITY] CVE-2010-2227: Apache Tomcat Remote Denial Of Service and Information Disclosure Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/512272/100/0/threaded>

* CONFIRM:

<http://svn.apache.org/viewvc?view=revision&revision=958911>

* CONFIRM:

<http://svn.apache.org/viewvc?view=revision&revision=958977>

* CONFIRM:

<http://svn.apache.org/viewvc?view=revision&revision=959428>

* CONFIRM:

<http://tomcat.apache.org/security-5.html>

* CONFIRM:

<http://tomcat.apache.org/security-6.html>

* CONFIRM:

<http://tomcat.apache.org/security-7.html>

* BID: 41544

<http://www.securityfocus.com/bid/41544>

* SECTRACK: 1024180

<http://securitytracker.com/id?1024180>

* XF: tomcat-transferencoding-dos(60264)

<http://xforce.iss.net/xforce/xfdb/60264>

CVE Reference:

CVE-2010-2227 (cve.mitre.org, nvd.nist.gov)

• 18874 Internet Explorer Event Handler Cross-Domain Vulnerability (MS10-053/2183461) (Remote File Checking)

An information disclosure vulnerability exists in Internet Explorer that could allow script to gain access to a browser window 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 then interacts with the browser window using the mouse.

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

References:

* MS: MS10-053

<http://www.microsoft.com/technet/security/bulletin/ms10-053.msp>

* BID: 42258

<http://www.securityfocus.com/bid/42258>

* VUPEN: VUPEN/ADV-2010-2050

<http://www.vupen.com/english/advisories/2010/2050>

* SECTRACK: 1024303

<http://securitytracker.com/alerts/2010/Aug/1024303.html>

CVE Reference:

CVE-2010-1258 (cve.mitre.org, nvd.nist.gov)

• 18875 Internet Explorer Uninitialized Memory Corruption Vulnerability (MS10-053/2183461) (CVE-2010-2556) (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:

* MS: MS10-053

<http://www.microsoft.com/technet/security/bulletin/ms10-053.msp>

* BID: 42257

<http://www.securityfocus.com/bid/42257>

* VUPEN: VUPEN/ADV-2010-2050

<http://www.vupen.com/english/advisories/2010/2050>

* SECTRACK: 1024303

<http://securitytracker.com/alerts/2010/Aug/1024303.html>

CVE Reference:

CVE-2010-2556 (cve.mitre.org, nvd.nist.gov)

• 18876 Internet Explorer Uninitialized Memory Corruption Vulnerability (MS10-053/2183461) (CVE-2010-2557) (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:

- * MS: MS10-053
<http://www.microsoft.com/technet/security/bulletin/ms10-053.msp>
- * BID: 42288
<http://www.securityfocus.com/bid/42288>
- * VUPEN: VUPEN/ADV-2010-2050
<http://www.vupen.com/english/advisories/2010/2050>
- * SECTRACK: 1024303
<http://securitytracker.com/alerts/2010/Aug/1024303.html>

CVE Reference:

CVE-2010-2557 (cve.mitre.org, nvd.nist.gov)

• 18877 Internet Explorer Race Condition Memory Corruption Vulnerability (MS10-053/2183461) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that may have been corrupted due to a race condition. 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:

- * MS: MS10-053
<http://www.microsoft.com/technet/security/bulletin/ms10-053.msp>
- * BID: 42289
<http://www.securityfocus.com/bid/42289>
- * VUPEN: VUPEN/ADV-2010-2050
<http://www.vupen.com/english/advisories/2010/2050>
- * SECTRACK: 1024303
<http://securitytracker.com/alerts/2010/Aug/1024303.html>

CVE Reference:

CVE-2010-2558 (cve.mitre.org, nvd.nist.gov)

• 18878 Internet Explorer Uninitialized Memory Corruption Vulnerability (MS10-053/2183461) (CVE-2010-2559) (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:

- * MS: MS10-053
<http://www.microsoft.com/technet/security/bulletin/ms10-053.msp>
- * BID: 42290
<http://www.securityfocus.com/bid/42290>
- * VUPEN: VUPEN/ADV-2010-2050
<http://www.vupen.com/english/advisories/2010/2050>

* SECTRACK: 1024303

<http://securitytracker.com/alerts/2010/Aug/1024303.html>

CVE Reference:

CVE-2010-2559 (cve.mitre.org, nvd.nist.gov)

• **18879 Internet Explorer HTML Layout Memory Corruption Vulnerability (MS10-053/2183461) (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:

* MS: MS10-053

<http://www.microsoft.com/technet/security/bulletin/ms10-053.msp>

* BID: 42292

<http://www.securityfocus.com/bid/42292>

* VUPEN: VUPEN/ADV-2010-2050

<http://www.vupen.com/english/advisories/2010/2050>

* SECTRACK: 1024303

<http://securitytracker.com/alerts/2010/Aug/1024303.html>

CVE Reference:

CVE-2010-2560 (cve.mitre.org, nvd.nist.gov)

• **18880 SMB Pool Overflow Vulnerability (MS10-054/982214) (Remote File Checking)**

An unauthenticated remote code execution vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the Server service. An attacker who successfully exploited this vulnerability could take complete control of the system.

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

References:

* MS: MS10-054

<http://www.microsoft.com/technet/security/bulletin/ms10-054.msp>

* BID: 42224

<http://www.securityfocus.com/bid/42224>

* VUPEN: VUPEN/ADV-2010-2051

<http://www.vupen.com/english/advisories/2010/2051>

* SECTRACK: 1024297

<http://securitytracker.com/alerts/2010/Aug/1024297.html>

CVE Reference:

CVE-2010-2550 (cve.mitre.org, nvd.nist.gov)

• **18881 SMB Variable Validation Vulnerability (MS10-054/982214) (Remote File Checking)**

A denial of service vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the Server service.

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

References:

* MS: MS10-054

<http://www.microsoft.com/technet/security/bulletin/ms10-054.msp>

* BID: 42263

<http://www.securityfocus.com/bid/42263>

* VUPEN: VUPEN/ADV-2010-2051

<http://www.vupen.com/english/advisories/2010/2051>

* SECTRACK: 1024297

<http://securitytracker.com/alerts/2010/Aug/1024297.html>

CVE Reference:

CVE-2010-2551 (cve.mitre.org, nvd.nist.gov)

• 18882 SMB Stack Exhaustion Vulnerability (MS10-054/982214) (Remote File Checking)

A denial of service vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB compounded requests. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the Server service.

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

References:

* MS: MS10-054

<http://www.microsoft.com/technet/security/bulletin/ms10-054.msp>

* BID: 42267

<http://www.securityfocus.com/bid/42267>

* VUPEN: VUPEN/ADV-2010-2051

<http://www.vupen.com/english/advisories/2010/2051>

* SECTRACK: 1024297

<http://securitytracker.com/alerts/2010/Aug/1024297.html>

CVE Reference:

CVE-2010-2552 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-2707 HP CVSS 2.0 Score = 8.3

Unspecified vulnerability on the HP ProCurve 2626 and 2650 switches before H.10.80 allows remote attackers to obtain sensitive information, modify data, and cause a denial of service via unknown vectors.

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

References:

SECUNIA: <http://secunia.com/advisories/40865>

HP: http://itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02436047

HP: http://itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02436047

CVE Reference: [CVE-2010-2707](http://cve.mitre.org)

• CVE-2010-2705 HP CVSS 2.0 Score = 6.1

Unspecified vulnerability on the HP ProCurve 1800-24G switch with software PB.03.02 and earlier, and the ProCurve 1800-8G switch with software PA.03.02 and earlier, when SNMP is enabled, allows remote attackers to obtain sensitive information via unknown vectors.

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

References:

HP: https://itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02436028

HP: https://itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02436028

SECUNIA: <http://secunia.com/advisories/40867>

CVE Reference: [CVE-2010-2705](http://cve.mitre.org)

• CVE-2010-2706 HP CVSS 2.0 Score = 6.1

Unspecified vulnerability in the In-band Agent on the HP ProCurve 2610 switch before R.11.30 allows remote attackers to cause a denial of service via unknown vectors.

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

References:

SECUNIA: <http://secunia.com/advisories/40864>

HP: http://itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02436043

HP: http://itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02436043

CVE Reference: [CVE-2010-2706](#)

• **CVE-2010-2708 HP CVSS 2.0 Score = 6.1**

Unspecified vulnerability on the HP ProCurve 2610 switch before R.11.22, when DHCP is enabled, allows remote attackers to cause a denial of service via unknown vectors.

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

References:

SECUNIA: <http://secunia.com/advisories/40864>

HP: http://itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02436045

HP: http://itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02436045

CVE Reference: [CVE-2010-2708](#)

• **CVE-2010-2976 Cisco CVSS 2.0 Score = 10.0**

The controller in Cisco Unified Wireless Network (UWN) Solution 7.x through 7.0.98.0 has (1) a default SNMP read-only community of public, (2) a default SNMP read-write community of private, and a value of "default" for the (3) SNMP v3 username, (4) SNMP v3 authentication password, and (5) SNMP v3 privacy password, which makes it easier for remote attackers to obtain access.

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

References:

CONFIRM: <http://www.cisco.com/en/US/docs/wireless/controller/release/notes/crn7.0.html>

CVE Reference: [CVE-2010-2976](#)

• **CVE-2010-2977 Cisco CVSS 2.0 Score = 10.0**

Cisco Unified Wireless Network (UWN) Solution 7.x before 7.0.98.0 does not properly implement TLS and SSL, which has unspecified impact and remote attack vectors, aka Bug ID CSCtd01611.

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

References:

CONFIRM: <http://www.cisco.com/en/US/docs/wireless/controller/release/notes/crn7.0.html>

CVE Reference: [CVE-2010-2977](#)

• **CVE-2010-2978 Cisco CVSS 2.0 Score = 10.0**

Cisco Unified Wireless Network (UWN) Solution 7.x before 7.0.98.0 does not use an adequate message-digest algorithm for a self-signed certificate, which allows remote attackers to bypass intended access restrictions via vectors involving collisions, aka Bug ID CSCtd67660.

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

References:

CONFIRM: <http://www.cisco.com/en/US/docs/wireless/controller/release/notes/crn7.0.html>

CVE Reference: [CVE-2010-2978](#)

• **CVE-2010-2984 Cisco CVSS 2.0 Score = 10.0**

Cisco Unified Wireless Network (UWN) Solution 7.x before 7.0.98.0 on 4404 series controllers does not properly implement the WEBAUTH_REQD state, which allows remote attackers to bypass intended access restrictions via WLAN traffic, aka Bug ID CSCtb75305.

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

References:

CONFIRM: <http://www.cisco.com/en/US/docs/wireless/controller/release/notes/crn7.0.html>

CVE Reference: [CVE-2010-2984](#)

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