ScoutNews
The weekly Security update from the makers of SecureScout
November 05, 2010

2010 Issue #44

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

Company sued for being slow reacting to breach. Microsoft sends out warning. New organization help identity theft victims.A new way of 'finger printing'.

The PCI Council has released PCI Data Security Standard (DSS) 2.0. This version includes mainly clarifying updates, there are no major changes. The old standard can be used until December 31th 2011.

netVigilance is preparing support for 64-bit operating systems, the 64-Bit netVigilance Internal Scan -Windows (NX) runs in our development lab without problems. New 64-bit installers are currently being build and tested, and will be based on Internal Scan - Windows version 2.6.442.0.

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

- **Indiana attorney general sues WellPoint over breach**

The Indiana attorney general's office has filed a lawsuit against Indianapolis-based health insurance provider WellPoint for taking months to notify state residents whose personal information was breached. The lawsuit, filed Friday, contends that WellPoint violated state law, which requires breached businesses to notify affected individuals and the attorney general's office "without reasonable delay," Attorney General Greg Zoeller said in a news release.

Zoeller said WellPoint learned of the breach, which affected more than 32,000 Indiana citizens, on Feb. 22, but did not begin notifying customers until almost four months later, on June 18.

After learning of the exposure through media reports, Zoeller's office tried to contact WellPoint, receiving a response in late July. SC Magazine

Full Story :
http://www.scmagazineus.com/indiana-attorney-general-sues-wellpoint-over-breach/article/190054/?utm_source=fee

- **Microsoft warns of targeted attacks using new IE hole**

E-mail sent to people in targeted organizations. Click for larger version.

(Credit: Symantec)

Microsoft today warned of a hole in older versions of Internet Explorer that was used in limited targeted attacks in which e-mails were sent to people in organizations directing them to a Web site where exploit code could take over their computers. Cnet Security

Full Story :
http://news.cnet.com/8301-27080_3-20021665-245.html?part=rss&subj=news&tag=2547-1_3-0-20

- **Identity Theft Council launches in Bay Area**

Neal O'Farrell, executive director of the Identity Theft Council

Victims of identity fraud should now have some extra help in the San Francisco Bay Area with a new grassroots organization, the Identity Theft Council.

The Identity Theft Council, which launched last week, is training volunteers at banks, credit unions, schools, law enforcement groups, and other organizations to work with consumers who have had their Social Security number, financial data, or other sensitive information pilfered. Theft of such information puts people at risk of having their names used for identity fraud. Cnet Security

Full Story :
http://news.cnet.com/8301-27080_3-20021700-245.html?part=rss&subj=news&tag=2547-1_3-0-20

- **PC typing errors can help guard against intruders**

IDG News Service - Hackers might crack or steal your password, but can they type like you?

Japan's NTT Communications has developed a computer security system that analyzes the way a computer user types, and then checks it against a profile of authorized users to detect if the person at the keyboard is an imposter.

The system, called Key Touch Pass, records the speed at which a user is typing, the length of time they typically hold down each key and the errors they normally make. Computerworld

Full Story :
http://www.computerworld.com/s/article/9194859/PC_typing_errors_can_help_guard_against_intruders?source=rss_

New Vulnerabilities Tested in SecureScout

- **18983 Negative Future Function Vulnerability (MS10-080/2293211) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. 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: MS10-080
http://www.microsoft.com/technet/security/Bulletin/MS10-080.mspx
* BID: 43653
http://www.securityfocus.com/bid/43653
* VUPEN: VUPEN/ADV-2010-2627
http://www.vupen.com/english/advisories/2010/2627
* SECTRACK: 1024552
http://securitytracker.com/alerts/2010/Oct/1024552.html

CVE Reference:

CVE-2010-3238 (cve.mitre.org, nvd.nist.gov)

- **18984 Extra Out of Boundary Record Parsing Vulnerability (MS10-080/2293211) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. 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: MS10-080
http://www.microsoft.com/technet/security/Bulletin/MS10-080.mspx
* BID: 43654
http://www.securityfocus.com/bid/43654
* VUPEN: VUPEN/ADV-2010-2627
http://www.vupen.com/english/advisories/2010/2627
* SECTRACK: 1024552
http://securitytracker.com/alerts/2010/Oct/1024552.html

CVE Reference:

CVE-2010-3239 (cve.mitre.org, nvd.nist.gov)

- **18985 Real Time Data Array Record Vulnerability (MS10-080/2293211) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. 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: MS10-080
http://www.microsoft.com/technet/security/Bulletin/MS10-080.mspx
* BID: 43655
http://www.securityfocus.com/bid/43655
* VUPEN: VUPEN/ADV-2010-2627
http://www.vupen.com/english/advisories/2010/2627
* SECTRACK: 1024552
http://securitytracker.com/alerts/2010/Oct/1024552.html

CVE Reference:

CVE-2010-3240 (cve.mitre.org, nvd.nist.gov)

- **18986 Out-of-Bounds Memory Write in Parsing Vulnerability (MS10-080/2293211) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. 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: MS10-080
http://www.microsoft.com/technet/security/Bulletin/MS10-080.mspx
* BID: 43656
http://www.securityfocus.com/bid/43656
* VUPEN: VUPEN/ADV-2010-2627
http://www.vupen.com/english/advisories/2010/2627
* SECTRACK: 1024552
http://securitytracker.com/alerts/2010/Oct/1024552.html

CVE Reference:

CVE-2010-3241 (cve.mitre.org, nvd.nist.gov)

- **18987 Ghost Record Type Parsing Vulnerability (MS10-080/2293211) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. 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: MS10-080
http://www.microsoft.com/technet/security/Bulletin/MS10-080.mspx
* BID: 43657
http://www.securityfocus.com/bid/43657
* VUPEN: VUPEN/ADV-2010-2627
http://www.vupen.com/english/advisories/2010/2627
* SECTRACK: 1024552
http://securitytracker.com/alerts/2010/Oct/1024552.html

CVE Reference:

CVE-2010-3242 (cve.mitre.org, nvd.nist.gov)

• 18988 Win32k Reference Count Vulnerability (MS10-073/981957) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that the Windows kernel-mode drivers maintain the reference count for an object. 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:

* NETVIGILANCE-UNKNOWN: 14156
http://www.exploit-db.com/exploits/14156
* FULLDISC: 20100630 MSRC-001: Windows Vista/Server 2008 NtUserCheckAccessForIntegrityLevel Use-after-free Vulnerability
http://seclists.org/fulldisclosure/2010/Jul/3
* BID: 41280
http://www.securityfocus.com/bid/41280
* OSVDB: 66003
http://osvdb.org/66003
* SECUNIA: 40421
http://secunia.com/advisories/40421
* XF: ms-win-ntusercheck-priv-escalation(60120)
http://xforce.iss.net/xforce/xfdb/60120
* SECTRACK: 1024547
http://securitytracker.com/alerts/2010/Oct/1024547.html
* VUPEN: VUPEN/ADV-2010-2620
http://www.vupen.com/english/advisories/2010/2620
* MS: MS10-073
http://www.microsoft.com/technet/security/bulletin/MS10-073.mspx

CVE Reference:

CVE-2010-2549 (cve.mitre.org, nvd.nist.gov)

• 18989 Win32k Keyboard Layout Vulnerability (MS10-073/981957) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that the Windows kernel-mode drivers load specific keyboard layouts. 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:

* MS: MS10-073
http://www.microsoft.com/technet/security/bulletin/MS10-073.mspx
* VUPEN: VUPEN/ADV-2010-2620
http://www.vupen.com/english/advisories/2010/2620
* BID: 43774
http://www.securityfocus.com/bid/43774
* SECTRACK: 1024547
http://securitytracker.com/alerts/2010/Oct/1024547.html

CVE Reference:

CVE-2010-2743 (cve.mitre.org, nvd.nist.gov)

- **18990 Win32k Window Class Vulnerability (MS10-073/981957) (Remote File Checking)**

An elevation of privilege vulnerability exists when the Windows kernel-mode drivers do not properly validate window class data. 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:

* MS: MS10-073
http://www.microsoft.com/technet/security/bulletin/MS10-073.mspx
* VUPEN: VUPEN/ADV-2010-2620
http://www.vupen.com/english/advisories/2010/2620
* BID: 43773
http://www.securityfocus.com/bid/43773
* SECTRACK: 1024547
http://securitytracker.com/alerts/2010/Oct/1024547.html

CVE Reference:

CVE-2010-2744 (cve.mitre.org, nvd.nist.gov)

- **18991 OpenType Font Parsing Vulnerability (MS10-078/2279986) (Remote File Checking)**

An elevation of privilege vulnerability exists in the way that the Windows OpenType Font (OTF) format driver improperly parses specially crafted OpenType fonts. 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-2010-2625
http://www.vupen.com/english/advisories/2010/2625
* BID: 43778
http://www.securityfocus.com/bid/43778
* SECTRACK: 1024554
http://securitytracker.com/alerts/2010/Oct/1024554.html
* MS: MS10-078
http://www.microsoft.com/technet/security/Bulletin/MS10-078.mspx

CVE Reference:

CVE-2010-2740 (cve.mitre.org, nvd.nist.gov)

- **18992 OpenType Font Validation Vulnerability (MS10-078/2279986) (Remote File Checking)**

An elevation of privilege vulnerability exists in the way that the Windows OpenType Font (OTF) format driver improperly parses specially crafted OpenType fonts. 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-2010-2625
http://www.vupen.com/english/advisories/2010/2625
* BID: 43779
http://www.securityfocus.com/bid/43779
* SECTRACK: 1024554
http://securitytracker.com/alerts/2010/Oct/1024554.html
* MS: MS10-078
http://www.microsoft.com/technet/security/Bulletin/MS10-078.mspx

CVE Reference:

CVE-2010-2741 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2010-4031 HP CVSS 2.0 Score = 8.0**

Unspecified vulnerability in HP Insight Control Performance Management before 6.2 allows remote authenticated users to gain privileges via unknown vectors.

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

References:

VUPEN: http://www.vupen.com/english/advisories/2010/2832

HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02563642

HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02563642

CVE Reference: CVE-2010-4031

- **CVE-2010-4032 HP CVSS 2.0 Score = 6.8**

Cross-site request forgery (CSRF) vulnerability in HP Insight Control Performance Management before 6.2 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.

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

References:

VUPEN: http://www.vupen.com/english/advisories/2010/2832

HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02563642

HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02563642

CVE Reference: CVE-2010-4032

- **CVE-2010-4106 HP CVSS 2.0 Score = 6.8**

Cross-site request forgery (CSRF) vulnerability in HP Insight Control for Linux before 6.2 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/62859

VUPEN: http://www.vupen.com/english/advisories/2010/2834

BID: http://www.securityfocus.com/bid/44537

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02573692

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02573692

SECUNIA: http://secunia.com/advisories/42040

CVE Reference: CVE-2010-4106

- **CVE-2010-4105 HP CVSS 2.0 Score = 6.4**

Unspecified vulnerability in HP Insight Orchestration before 6.2 allows remote attackers to bypass intended access restrictions, and obtain sensitive information or modify data, via unknown vectors.

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

References:

VUPEN: http://www.vupen.com/english/advisories/2010/2829

BID: http://www.securityfocus.com/bid/44534

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02573285

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02573285

SECUNIA: http://secunia.com/advisories/42036

CVE Reference: CVE-2010-4105

- **CVE-2010-4100 HP CVSS 2.0 Score = 5.0**

Unspecified vulnerability in HP Insight Control Performance Management before 6.1 update 2 allows remote attackers to read arbitrary files via unknown vectors.

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

References:

VUPEN: http://www.vupen.com/english/advisories/2010/2833

HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02574359

HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02574359

CVE Reference: CVE-2010-4100

- **CVE-2010-4102 HP CVSS 2.0 Score = 5.0**

Unspecified vulnerability in HP Insight Recovery before 6.2 allows remote attackers to read arbitrary files via unknown vectors.

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

References:

VUPEN: http://www.vupen.com/english/advisories/2010/2830

BID: http://www.securityfocus.com/bid/44542

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02571464

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02571464

SECUNIA: http://secunia.com/advisories/42037

CVE Reference: CVE-2010-4102

- **CVE-2010-4103 HP CVSS 2.0 Score = 5.0**

Unspecified vulnerability in HP Insight Managed System Setup Wizard before 6.2 allows remote attackers to read arbitrary files via unknown vectors.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/62860

VUPEN: http://www.vupen.com/english/advisories/2010/2831

BID: http://www.securityfocus.com/bid/44532

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02573176

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02573176

SECUNIA: http://secunia.com/advisories/42038

CVE Reference: CVE-2010-4103

- **CVE-2010-4104 HP CVSS 2.0 Score = 5.0**

Unspecified vulnerability in HP Insight Orchestration before 6.2 allows remote attackers to read arbitrary files via unknown vectors.

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

References:

VUPEN: http://www.vupen.com/english/advisories/2010/2829

BID: http://www.securityfocus.com/bid/44534

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02573285

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02573285

SECUNIA: http://secunia.com/advisories/42036

CVE Reference: CVE-2010-4104

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