

## 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

Industry asked to comment on PCI DSS improvements. Open source soaring during recession. Securing the home office. A new view on cheating needed.

Enjoy reading & Stay safe.

**Call or email netVigilance to get an update on SecureScout.**

**(503) 524 5758 or [sales@netvigilance.com](mailto:sales@netvigilance.com)**

## Top Security News Stories this Week

### • PCI Security Council seeks industry comments on current standards

Computerworld - The group that administers the Payment Card Industry Data Security Standard (PCI DSS) wants feedback about how the current version of the standard, released last October, is working.

Retailers, financial institutions and others in the payment industry will be able to submit online comments between July 1 and Nov. 1 about how to improve the PCI DSS 1.2 standard, the PCI Security Standards Council (SSC) said this week. Over the next few months, the PCI SSC will hold two "community meetings" -- one in the U.S., the other in Europe -- where stakeholders can also weigh in. Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9134859>

### • Red Hat: Bad economy is good for open source

For those wondering whether Oracle or Red Hat is weathering the recession best, this week may have settled the question. On Tuesday the market cheered Oracle for only seeing a 5.2 percent drop in revenue, with a 7.2 percent drop in profit (absent the strong dollar, Oracle would have seen a 4 percent increase in revenue and a 5 percent increase in profit).

Red Hat? Well, on Wednesday Red Hat announced fiscal first-quarter revenue of \$174 million, up 11 percent from the prior year. Subscription revenue was up 14 percent year over year to \$148.8 million. The company's total deferred revenue balance is now \$567.3 million, an increase of 15 percent on a year-over-year basis. Net income for the quarter was \$18.5 million.

Both Oracle and Red Hat are doing well, and Oracle is obviously dealing with much bigger wads of money, but it seems clear that Red Hat's open-source model is the big winner in the recession. Cnet Security

Full Story :

[http://news.cnet.com/8301-13505\\_3-10272310-16.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-13505_3-10272310-16.html?part=rss&subj=news&tag=2547-1_3-0-20)

### • **Seven Deadly Sins of Home Office Security**

CSO - According to the human resources association World at Work, 17.2 million Americans worked from home or remotely at least one day per month for their employer last year (See also: 4 Telecommuting Security Mistakes). And the 2007 book 'Microtrends' estimates that 4.2 million Americans work full-time from home.

Good security is a key to good productivity. CSO spoke with two home office security experts about security mistakes home office workers often make (and how to avoid those errors).

Failing to physically secure the office Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9134648>

### • **Kids cheating with tech but are schools cheating kids?**

The results of a survey showing that 35 percent of middle school and high school students with cell phones have used them to cheat at school is indeed alarming. And perhaps more alarming is the finding that nearly a quarter of the students don't even think it's cheating.

Cheating is cheating regardless of whether you use technology or old-fashioned paper notes. I'm appalled that kids may be using technology to cheat in school, but I'm just as appalled at how schools are cheating kids when it comes to technology.

But in addition to admonishing kids about why it's wrong to cheat, perhaps it's also time to rethink what it means to evaluate students in the age of the Internet and omnipresent mobile devices. Cnet Security

Full Story :

[http://news.cnet.com/8301-19518\\_3-10270987-238.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-19518_3-10270987-238.html?part=rss&subj=news&tag=2547-1_3-0-20)

### • **ICANN: New domains coming in 2010**

Network World - Internet policymakers are forging ahead with a controversial plan to introduce hundreds of generic top-level domains -- such as .nyc, .sport and .food -- next year.

However, U.S. corporations with large portfolios of domain names are still pushing for a go-slow approach and more protection for trademark owners to prevent cybersquatting and other deceptive practices such as phishing.

In addition, leading registries are arguing for the continued separation of back-end and retail domain name operations. ICANN also faces criticism about the fees it plans to charge new gTLD applicants. Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9134766>

## **New Vulnerabilities Tested in SecureScout**

### • **18418 Word Buffer Overflow Vulnerability (CVE-2009-0563) (MS09-027/969514) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office Word handles a specially crafted Word file that includes a malformed record. 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

#### References:

- \* BUGTRAQ: 20090610 ZDI-09-035: Microsoft Word Document Stack Based Buffer Overflow Vulnerability  
<http://www.securityfocus.com/archive/1/archive/1/504204/100/0/threaded>
- \* MISC:  
<http://www.zerodayinitiative.com/advisories/ZDI-09-035>
- \* MS: MS09-027  
<http://www.microsoft.com/technet/security/Bulletin/MS09-027.msp>
- \* BID: 35188  
<http://www.securityfocus.com/bid/35188>
- \* OSVDB: 54959  
<http://osvdb.org/54959>
- \* SECTRACK: 1022356  
<http://www.securitytracker.com/id?1022356>
- \* VUPEN: ADV-2009-1546  
<http://www.vupen.com/english/advisories/2009/1546>

#### CVE Reference:

CVE-2009-0563 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18419 Word Buffer Overflow Vulnerability (CVE-2009-0565) (MS09-027/969514) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Word handles a specially crafted Word file that includes a malformed record. 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

#### References:

- \* MS: MS09-027  
<http://www.microsoft.com/technet/security/Bulletin/MS09-027.msp>
- \* BID: 35190  
<http://www.securityfocus.com/bid/35190>
- \* OSVDB: 54960  
<http://osvdb.org/54960>
- \* SECTRACK: 1022356  
<http://www.securitytracker.com/id?1022356>
- \* VUPEN: ADV-2009-1546  
<http://www.vupen.com/english/advisories/2009/1546>

#### CVE Reference:

CVE-2009-0565 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18428 RPC Marshalling Engine Vulnerability (MS09-026/970238) (Remote File Checking)

An elevation of privilege vulnerability exists in the Windows remote procedure call (RPC) facility where the RPC Marshalling Engine does not update its internal state appropriately. The failure to update internal state could lead to a pointer being read from an incorrect location. An attacker who successfully exploited this vulnerability could execute arbitrary code and 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:

- \* CONFIRM:  
<http://blogs.technet.com/srd/archive/2009/06/09/ms09-026-how-a-developer-can-know-if-their-rpc-interface-is-affected.aspx>
- \* MS: MS09-026  
<http://www.microsoft.com/technet/security/Bulletin/MS09-026.msp>
- \* BID: 35219  
<http://www.securityfocus.com/bid/35219>
- \* OSVDB: 54936  
<http://osvdb.org/54936>
- \* SECTRACK: 1022357  
<http://www.securitytracker.com/id?1022357>

\* VUPEN: ADV-2009-1545

<http://www.vupen.com/english/advisories/2009/1545>

#### CVE Reference:

CVE-2009-0568 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18429 Windows Kernel Desktop Vulnerability (MS09-025/968537) (Remote File Checking)

An elevation of privilege vulnerability exists in the way that the Windows kernel does not properly validate changes in certain kernel objects. 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: MS09-025

<http://www.microsoft.com/technet/security/Bulletin/MS09-025.msp>

\* OSVDB: 54940

<http://osvdb.org/54940>

\* SECTRACK: 1022359

<http://www.securitytracker.com/id?1022359>

\* SECUNIA: 35372

<http://secunia.com/advisories/35372>

\* VUPEN: ADV-2009-1544

<http://www.vupen.com/english/advisories/2009/1544>

#### CVE Reference:

CVE-2009-1123 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18430 Windows Kernel Pointer Validation Vulnerability (MS09-025/968537) (Remote File Checking)

An elevation of privilege vulnerability exists in the Windows kernel due to the insufficient validation of certain pointers passed from user mode. 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: MS09-025

<http://www.microsoft.com/technet/security/Bulletin/MS09-025.msp>

\* BID: 35238

<http://www.securityfocus.com/bid/35238>

\* OSVDB: 54941

<http://osvdb.org/54941>

\* SECTRACK: 1022359

<http://www.securitytracker.com/id?1022359>

\* SECUNIA: 35372

<http://secunia.com/advisories/35372>

\* VUPEN: ADV-2009-1544

<http://www.vupen.com/english/advisories/2009/1544>

#### CVE Reference:

CVE-2009-1124 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18431 Windows Driver Class Registration Vulnerability (MS09-025/968537) (Remote File Checking)

An elevation of privilege vulnerability exists because the Windows kernel does not properly validate an argument passed to a Windows kernel system call. 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: MS09-025

<http://www.microsoft.com/technet/security/Bulletin/MS09-025.msp>

\* BID: 35240

<http://www.securityfocus.com/bid/35240>

\* OSVDB: 54942  
<http://osvdb.org/54942>  
\* SECTRACK: 1022359  
<http://www.securitytracker.com/id?1022359>  
\* SECUNIA: 35372  
<http://secunia.com/advisories/35372>  
\* VUPEN: ADV-2009-1544  
<http://www.vupen.com/english/advisories/2009/1544>

**CVE Reference:**

CVE-2009-1125 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18432 Windows Desktop Parameter Edit Vulnerability (MS09-025/968537) (Remote File Checking)**

An elevation of privilege vulnerability exists when the Windows kernel improperly validates input passed from user mode to the kernel when editing a specific desktop parameter. The vulnerability could allow an attacker to run code with elevated privileges. 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: MS09-025  
<http://www.microsoft.com/technet/security/Bulletin/MS09-025.mspx>  
\* OSVDB: 54943  
<http://osvdb.org/54943>  
\* SECTRACK: 1022359  
<http://www.securitytracker.com/id?1022359>  
\* SECUNIA: 35372  
<http://secunia.com/advisories/35372>  
\* VUPEN: ADV-2009-1544  
<http://www.vupen.com/english/advisories/2009/1544>

**CVE Reference:**

CVE-2009-1126 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18433 IIS 5.0 WebDAV Authentication Bypass Vulnerability (MS020/970483) (Remote File Checking)**

An elevation of privilege vulnerability exists in the way that the WebDAV extension for IIS handles HTTP requests. An attacker could exploit this vulnerability by creating a specially crafted anonymous HTTP request to gain access to a location that should require authentication.

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

**References:**

\* MS: MS09-020  
<http://www.microsoft.com/technet/security/Bulletin/MS09-020.mspx>  
\* BID: 35232  
<http://www.securityfocus.com/bid/35232>  
\* SECTRACK: 1022358  
<http://www.securitytracker.com/id?1022358>  
\* VUPEN: ADV-2009-1539  
<http://www.vupen.com/english/advisories/2009/1539>

**CVE Reference:**

CVE-2009-1122 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18434 IIS 5.1 and 6.0 WebDAV Authentication Bypass Vulnerability (MS020/970483) (Remote File Checking)**

An elevation of privilege vulnerability exists in the way that the WebDAV extension for IIS handles HTTP requests. An attacker could exploit this vulnerability by creating a specially crafted anonymous HTTP request to gain access to a location that typically requires authentication.

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

**References:**

\* FULLDISC: 20090515 IIS6 webdav and unicode rides again in 2009  
<http://archives.neohapsis.com/archives/fulldisclosure/2009-05/0135.html>  
\* FULLDISC: 20090515 Re: IIS6 webdav and unicode rides again in 2009  
<http://archives.neohapsis.com/archives/fulldisclosure/2009-05/0144.html>  
\* FULLDISC: 20090515 Re: IIS6 webdav and unicode rides again in 2009  
<http://archives.neohapsis.com/archives/fulldisclosure/2009-05/0139.html>  
\* MISC:  
[http://archives.neohapsis.com/archives/fulldisclosure/2009-05/att-0135/IIS\\_Advisory.pdf](http://archives.neohapsis.com/archives/fulldisclosure/2009-05/att-0135/IIS_Advisory.pdf)  
\* MISC:  
<http://blog.zoller.lu/2009/05/iis-6-webdac-auth-bypass-and-data.html>  
\* MISC:  
<http://isc.sans.org/diary.html?n&storyid=6397>  
\* MISC:  
<http://view.samurajdata.se/psview.php?id=023287d6&page=1>  
\* MS: MS09-020  
<http://www.microsoft.com/technet/security/Bulletin/MS09-020.msp>

#### CVE Reference:

CVE-2009-1535 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18436 Unencrypted Firewall-1 Web Management Access Vulnerability

Firewall-1 Web Access Port (CheckPoint) is the remote user access/auth port via browser (http). It is an alternative to telnet to FW's tcp 259. Via a browser connection the user can authenticate and use all permitted web resources of the internal network.

The access to the remote user access/auth port is not encrypted.

PCI DSS version 1.2 Requirement 2.3 specifies that all non-console administrative access be encrypted. It is recommended to use technologies such as SSH, VPN, or SSL/TLS for webbased management and other non-console administrative access in order to secure access to these consoles.

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

#### References:

\* MISC: About the PCI Data Security Standard (PCI DSS)  
[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)

#### CVE Reference:

## New Vulnerabilities found this Week

#### • CVE-2009-0903 IBM CVSS 2.0 Score = 7.5

IBM WebSphere Application Server (WAS) 7.0 before 7.0.0.3, and the Feature Pack for Web Services for WAS 6.1 before 6.1.0.25, when a WS-Security policy is established at the operation level, does not properly handle inbound requests that lack a SOAPAction or WS-Addressing Action, which allows remote attackers to bypass intended access restrictions via a crafted request to a JAX-WS application.

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

#### References:

AIXAPAR: <http://www-1.ibm.com/support/docview.wss?uid=swg1PK87767>

AIXAPAR: <http://www-1.ibm.com/support/docview.wss?uid=swg1PK81944>

XF: <http://xforce.iss.net/xforce/xfdb/51293>

#### CVE Reference: [CVE-2009-0903](http://cve.mitre.org/cve/2009/0903)

#### • CVE-2009-1163 Cisco CVSS 2.0 Score = 7.8

Memory leak on the Cisco Physical Access Gateway with software before 1.1 allows remote attackers to cause a denial of service (memory consumption) via unspecified TCP packets.

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

#### References:

CISCO: [http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080ad0f8b.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080ad0f8b.shtml)

**CVE Reference:** [CVE-2009-1163](#)

• **CVE-2009-2045 Cisco CVSS 2.0 Score = 7.8**

The Cisco Video Surveillance Stream Manager firmware before 5.3, as used on Cisco Video Surveillance Services Platforms and Video Surveillance Integrated Services Platforms, allows remote attackers to cause a denial of service (reboot) via a malformed payload in a UDP packet to port 37000, related to the xvcrman process, aka Bug ID CSCsj47924.

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

**References:**

CISCO: [http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080ad0f8f.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080ad0f8f.shtml)

**CVE Reference:** [CVE-2009-2045](#)

• **CVE-2009-2046 Cisco CVSS 2.0 Score = 6.8**

The embedded web server on the Cisco Video Surveillance 2500 Series IP Camera with firmware before 2.1 allows remote attackers to read arbitrary files via a (1) http or (2) https request, related to the (a) SD Camera Web Server and the (b) Wireless Camera HTTP Server, aka Bug IDs CSCsu05515 and CSCsr96497.

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

**References:**

CISCO: [http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080ad0f8f.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080ad0f8f.shtml)

**CVE Reference:** [CVE-2009-2046](#)

• **CVE-2009-1202 Cisco CVSS 2.0 Score = 4.3**

WebVPN on the Cisco Adaptive Security Appliances (ASA) device with software 8.0(4), 8.1.2, and 8.2.1 allows remote attackers to bypass certain protection mechanisms involving URL rewriting and HTML rewriting, and conduct cross-site scripting (XSS) attacks, by modifying the first hex-encoded character in a /+CSCO+ URI, aka Bug ID CSCsy80705.

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

**References:**

BID: <http://www.securityfocus.com/bid/35480>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/504516/100/0/threaded>

**CVE Reference:** [CVE-2009-1202](#)

• **CVE-2009-1201 Cisco CVSS 2.0 Score = 3.5**

Eval injection vulnerability in the cscowrap.js function in /+CSCOL+/cte.js in WebVPN on the Cisco Adaptive Security Appliances (ASA) device with software 8.0(4), 8.1.2, and 8.2.1 allows remote attackers to bypass a DOM wrapper and conduct cross-site scripting (XSS) attacks by setting CSCO\_WebVPN['process'] to the name of a crafted function, aka Bug ID CSCsy80694.

Test Case Impact: Vulnerability Impact: Risk: **Low**

**References:**

MISC: <https://www.trustwave.com/spiderlabs/advisories/TWSL2009-002.txt>

BID: <http://www.securityfocus.com/bid/35476>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/504516/100/0/threaded>

**CVE Reference:** [CVE-2009-1201](#)

• **CVE-2009-1860 Adobe CVSS 2.0 Score = 9.3**

Unspecified vulnerability in Adobe Shockwave Player before 11.5.0.600 allows remote attackers to execute arbitrary code via crafted Shockwave Player 10 content.

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

**References:**

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb09-08.html>

BID: <http://www.securityfocus.com/bid/35469>

SECUNIA: <http://secunia.com/advisories/35544>

**CVE Reference:** [CVE-2009-1860](#)

• **CVE-2009-2186 Adobe CVSS 2.0 Score = 9.3**

Unspecified vulnerability in Adobe Shockwave Player before 11.0.0.465 allows remote attackers to execute arbitrary code via unknown vectors, a different vulnerability than CVE-2009-1860.

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

**References:**

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb09-08.html>

**CVE Reference:** [CVE-2009-2186](#)

**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](mailto: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](mailto: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](mailto:info-scanner@securescout.net)