

## 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

[Sasser Worm Scanner](#) - The S4 Sasser Worm 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 Microsoft SSL Vulnerability (MS04-011) that used by the Sasser Worm to infect machines.

Download Here:

<http://www.netvigilance.com/productdownloads?productname=sasserwormscanner>

## This Week in Review

SOA in it's early stages with good security. Doing IT security under a strained budget. Number of ID stealing malware exploding. The most offensive website contains 18K different malwares.

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

### • SOA Security: Good Enough and Getting Better

CIO - Security is not a reason to stay away from SOA. Although full SOA security maturity is yet to come, 30 percent of organizations now use SOA for external integration with customers and partners. For standard Web services using SOAP, WS-Security has achieved critical mass as a foundational standard. On the other hand, advanced SOA security - involving federation among partners, nonrepudiation, and propagation of user identities across multiple layers of service implementations - is in its early days. To navigate the path from what's practical today to the future of advanced SOA security, establish an iterative design process for evolving your SOA security architecture that considers your current and future security requirements, emerging industry specifications, overlaps in product functionality for SOA security, and possibilities for custom security integration.

MORE ON SOA SOA Security: the Basics SOA Definition and Solutions SOA Security: How Irish Luck Went a Long Way Are you Insecure about SOA Security? Computerworld

Full Story :

[http://www.computerworld.com/s/article/9136843/SOA\\_Security\\_Good\\_Enough\\_and\\_Getting\\_Better?source=rss\\_sec](http://www.computerworld.com/s/article/9136843/SOA_Security_Good_Enough_and_Getting_Better?source=rss_sec)

- **Managed security services all the rage**

Network World - It's an understatement to say that IT organizations face exceptionally challenging times. For many, budget cutbacks for 2009 were worse than predicted. &#160;

12 managed security-services providers you should know

As a result, many IT organizations are taking a hard look at what is and is not core to internal IT, assessing their teams and moving people to strategic areas to concentrate on more important projects. Even organizations that traditionally kept services in-house are assessing whether to selectively outsource day-to-day monitoring and management to third parties in order to take advantage of the predictable monthly expense that managed services offer. Security managed services are no exception. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9136830/Managed\\_security\\_services\\_all\\_the\\_rage?source=rss\\_security](http://www.computerworld.com/s/article/9136830/Managed_security_services_all_the_rage?source=rss_security)

- **Malware designed to steal IDs increased 600 percent**

The number of users victimized by malware specifically intended to rob personally identifiable information (PII) leapt 600 percent this year compared to the same period in 2008, according to a report released on Thursday by PandaLabs, a division of Bilbao, Spain-based Panda Security.

&nbsp;

Writing on the PandaLabs blog, Luis Corrons, PandaLabs' director, said that of the nearly 37,000 samples of new viruses, worms, trojans and other types of internet threats PandaLabs receives each day, 71 percent are trojans, the majority of which are intended to siphon bank details or credit card numbers, as well as passwords for other commercial services. SC Magazine

Full Story :

<http://www.scmagazineus.com/Malware-designed-to-steal-IDs-increased-600-percent/article/146909/>

- **"Dirtiest" websites host average 18,000 threats**

The most dangerous sites on the web are propagating an average of 18,000 different pieces of malware, according to Symantec.

The security vendor on Wednesday put out a list of the most offensive sites on the web -- those hosting the most malware. As can be expected, 48 of the top 100 worst are adult-themed sites, but others&nbsp;featured diverse topics, ranging from deer hunting and catering, to figure skating, electronics and legal services.

Forty of the sites had more than 20,000 threats, according to Symantec. The most offensive site was propagating 56,371 viruses. And, three quarters of the sites on the list have been propagating malware for more than six months. SC Magazine

Full Story :

<http://www.scmagazineus.com/Dirtiest-websites-host-average-18000-threats/article/146919/>

- **Alleged data-heist kingpin is a computer addict, lawyer says**

Computerworld - Albert Gonzalez, the man described by federal authorities as the kingpin of a gang responsible for stealing more than 130 million payment cards, is a computer addict constantly looking for ways to challenge his abilities, according to his lawyer.

In a conversation with Computerworld on Wednesday, Rene Palomino, the Miami-based lawyer representing Gonzalez, said his client has had an unhealthy obsession with computers since the age of 8. However, he stopped short of saying it was this obsession that might have pushed Gonzalez to allegedly get involved with the crimes.

"He was self-taught," Palomino said of Gonzalez. "He didn't go out in the sandbox or play baseball. The computer was his best friend." Computerworld

Full Story :

[http://www.computerworld.com/s/article/9136917/Alleged\\_data\\_heist\\_kingpin\\_is\\_a\\_computer\\_addict\\_lawyer\\_says?s](http://www.computerworld.com/s/article/9136917/Alleged_data_heist_kingpin_is_a_computer_addict_lawyer_says?s)

## **New Vulnerabilities Tested in SecureScout**

- **18472 Windows Media File Processing Malformed AVI Header Vulnerability (MS09-038/971557) (Remote File Checking)**

A remote code execution vulnerability exists in the way Microsoft Windows handles specially crafted AVI format files. This vulnerability could allow code execution if a user opened a specially crafted AVI file. 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. 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: MS09-038  
<http://www.microsoft.com/technet/security/Bulletin/MS09-038.msp>
- \* BID: 35967  
<http://www.securityfocus.com/bid/35967>
- \* SECTrack: 1022711  
<http://www.securitytracker.com/id?1022711>
- \* SECUNIA: 36206  
<http://secunia.com/advisories/36206>
- \* VUPEN: ADV-2009-2233  
<http://www.vupen.com/english/advisories/2009/2233>

#### CVE Reference:

CVE-2009-1545 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18473 Windows Media File Processing AVI Integer Overflow Vulnerability (MS09-038/971557) (Remote File Checking)

A remote code execution vulnerability exists in the way Microsoft Windows handles specially crafted AVI format files. This vulnerability could allow code execution if a user opened a specially crafted AVI file. 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. 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: MS09-038  
<http://www.microsoft.com/technet/security/Bulletin/MS09-038.msp>
- \* BID: 35970  
<http://www.securityfocus.com/bid/35970>
- \* OSVDB: 56909  
<http://osvdb.org/56909>
- \* SECTrack: 1022711  
<http://www.securitytracker.com/id?1022711>
- \* SECUNIA: 36206  
<http://secunia.com/advisories/36206>
- \* VUPEN: ADV-2009-2233  
<http://www.vupen.com/english/advisories/2009/2233>

#### CVE Reference:

CVE-2009-1546 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18474 Microsoft Video ActiveX Control Vulnerability (MS09-037/973908) (Remote File Checking)

A remote code execution vulnerability exists in the Microsoft Active Template Library (ATL) due to the function CComVariant::ReadFromStream used in the ATL header. This function does not properly restrict untrusted data read from a stream. This issue leads to reading data directly onto the stack instead of reading it into the area of memory allocated for an array, which could allow a remote, unauthenticated user to perform remote code execution on an affected system. 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.

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

#### References:

- \* ISS: 20090706 Multiple Microsoft Video Control ActiveX Remote Code Execution Vulnerabilities  
<http://www.iss.net/threats/329.html>
- \* MISC:  
<http://isc.sans.org/diary.html?storyid=6733>

\* MISC:  
<http://www.csis.dk/dk/nyheder/nyheder.asp?tekstID=799>  
\* MISC:  
<http://blogs.technet.com/srd/archive/2009/08/11/ms09-037-why-we-are-using-cve-s-already-used-in-ms09-035.aspx>  
\* CONFIRM:  
<http://www.microsoft.com/technet/security/advisory/972890.msp>  
\* MS: MS09-032  
<http://www.microsoft.com/technet/security/Bulletin/MS09-032.msp>  
\* MS: MS09-037  
<http://www.microsoft.com/technet/security/Bulletin/MS09-037.msp>  
\* CERT: TA09-187A  
<http://www.us-cert.gov/cas/techalerts/TA09-187A.html>  
\* CERT-VN: VU#180513  
<http://www.kb.cert.org/vuls/id/180513>  
\* BID: 35558  
<http://www.securityfocus.com/bid/35558>  
\* BID: 35585  
<http://www.securityfocus.com/bid/35585>  
\* OSVDB: 55651  
<http://osvdb.org/55651>  
\* SECTRAK: 1022514  
<http://www.securitytracker.com/id?1022514>  
\* SECUNIA: 36187  
<http://secunia.com/advisories/36187>  
\* VUPEN: ADV-2009-2232  
<http://www.vupen.com/english/advisories/2009/2232>

#### CVE Reference:

CVE-2008-0015 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18475 ATL Header Memcopy Vulnerability (MS09-037/973908) (Remote File Checking)

A remote code execution vulnerability exists in the Microsoft Active Template Library (ATL) due to an error in the Load method of the IPersistStreamInit interface. The Load method could allow calls to memcpy with untrusted data, which could allow a remote, unauthenticated user to perform remote code execution on an affected system. 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.

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

#### References:

\* ISS: 20090706 Multiple Microsoft Video Control ActiveX Remote Code Execution Vulnerabilities  
<http://www.iss.net/threats/329.html>  
\* MISC:  
<http://blogs.technet.com/srd/archive/2009/08/11/ms09-037-why-we-are-using-cve-s-already-used-in-ms09-035.aspx>  
\* MS: MS09-037  
<http://www.microsoft.com/technet/security/Bulletin/MS09-037.msp>  
\* SECTRAK: 1022712  
<http://www.securitytracker.com/id?1022712>  
\* SECUNIA: 36187  
<http://secunia.com/advisories/36187>  
\* VUPEN: ADV-2009-2232  
<http://www.vupen.com/english/advisories/2009/2232>

#### CVE Reference:

CVE-2008-0020 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18476 ATL Uninitialized Object Vulnerability (MS09-037/973908) (Remote File Checking)

A remote code execution vulnerability exists in the Microsoft Active Template Library (ATL) due to a bug in the ATL headers that could allow an attacker to force VariantClear to be called on a VARIANT that has not been correctly initialized. Because of this bug, the attacker can control what happens when VariantClear is called during handling of an error by supplying a corrupt stream. This vulnerability only directly affects systems with components and controls installed that were built using Visual Studio ATL. This vulnerability could allow a remote, unauthenticated user to perform remote code execution on an affected system. 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.

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

#### References:

\* MISC:

<http://blogs.technet.com/srd/archive/2009/08/11/ms09-037-why-we-are-using-cve-s-already-used-in-ms09-035.aspx>

\* CONFIRM:

<http://www.adobe.com/support/security/advisories/apsa09-04.html>

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb09-11.html>

\* MS: MS09-035

<http://www.microsoft.com/technet/security/bulletin/ms09-035.msp>

\* MS: MS09-037

<http://www.microsoft.com/technet/security/Bulletin/MS09-037.msp>

\* BID: 35832

<http://www.securityfocus.com/bid/35832>

\* SECUNIA: 36187

<http://secunia.com/advisories/36187>

\* VUPEN: ADV-2009-2034

<http://www.vupen.com/english/advisories/2009/2034>

\* VUPEN: ADV-2009-2232

<http://www.vupen.com/english/advisories/2009/2232>

#### CVE Reference:

CVE-2009-0901 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18477 ATL COM Initialization Vulnerability (MS09-037/973908) (Remote File Checking)

A remote code execution vulnerability exists in the Microsoft Active Template Library (ATL) due to bugs in the ATL headers that handle instantiation of an object from data streams. This vulnerability only directly affects systems with components and controls installed that were built using Visual Studio ATL. For components and controls built using ATL, unsafe usage of OleLoadFromStream could allow the instantiation of arbitrary objects which can bypass related security policy, such as kill bits within Internet Explorer. This vulnerability could allow a remote, unauthenticated user to perform remote code execution on an affected system. 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.

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

#### References:

\* MISC:

<http://blogs.technet.com/srd/archive/2009/08/11/ms09-037-why-we-are-using-cve-s-already-used-in-ms09-035.aspx>

\* CONFIRM:

<http://www.adobe.com/support/security/advisories/apsa09-04.html>

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb09-11.html>

\* MS: MS09-035

<http://www.microsoft.com/technet/security/bulletin/ms09-035.msp>

\* MS: MS09-037

<http://www.microsoft.com/technet/security/Bulletin/MS09-037.msp>

\* SUNALERT: 264648

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-264648-1>

\* SECUNIA: 36187

<http://secunia.com/advisories/36187>

\* VUPEN: ADV-2009-2034

<http://www.vupen.com/english/advisories/2009/2034>

\* VUPEN: ADV-2009-2232

<http://www.vupen.com/english/advisories/2009/2232>

#### CVE Reference:

CVE-2009-2493 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18478 ATL Object Type Mismatch Vulnerability (MS09-037/973908) (Remote File Checking)

A remote code execution vulnerability exists in the Microsoft Active Template Library (ATL) due to a bug in the ATL header that could allow reading a variant from a stream and leaving the variant type read with an invalid variant. When deleting the variant, it is possible to free unintended areas in memory that could be controlled by an attacker.

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

#### References:

\* MISC:

<http://blogs.technet.com/srd/archive/2009/08/11/ms09-037-why-we-are-using-cve-s-already-used-in-ms09-035.aspx>

\* MS: MS09-037

<http://www.microsoft.com/technet/security/Bulletin/MS09-037.msp>

\* BID: 35982

<http://www.securityfocus.com/bid/35982>

\* OSVDB: 56910

<http://osvdb.org/56910>

\* SECTrack: 1022712

<http://www.securitytracker.com/id?1022712>

\* SECUNIA: 36187

<http://secunia.com/advisories/36187>

\* VUPEN: ADV-2009-2232

<http://www.vupen.com/english/advisories/2009/2232>

#### CVE Reference:

CVE-2009-2494 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18479 Workstation Service Memory Corruption Vulnerability (MS09-041/971657) (Remote File Checking)

An elevation of privilege vulnerability exists in the Windows Workstation Service due to a possible "Double Free" condition occurring in the service. An attacker who successfully exploited this vulnerability could run arbitrary code with elevated privileges. 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: MS09-041

<http://www.microsoft.com/technet/security/Bulletin/MS09-041.msp>

\* BID: 35972

<http://www.securityfocus.com/bid/35972>

#### CVE Reference:

CVE-2009-1544 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18480 Windows Message Queuing service Null Pointer Vulnerability (MS09-040/971032) (Remote File Checking)

An elevation of privilege vulnerability exists in the Windows Message Queuing service (MSMQ) due to a specific flaw in the parsing of an IOCTL request to the Message Queuing service. The MSMQ service improperly checks input data before passing them to the buffer. 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:

\* BUGTRAQ: 20090812 [PT-2008-09] Microsoft Windows MSMQ Privilege Escalation Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/505691/100/0/threaded>

\* MISC:

<http://en.securitylab.ru/lab/PT-2008-09>

\* MS: MS09-040

<http://www.microsoft.com/technet/security/Bulletin/MS09-040.msp>

\* OSVDB: 56901

<http://osvdb.org/56901>

\* SECTrack: 1022714

<http://www.securitytracker.com/id?1022714>

\* SECUNIA: 36214

<http://secunia.com/advisories/36214>

#### CVE Reference:

CVE-2009-1922 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18482 Telnet Credential Reflection Vulnerability (MS09-042/960859) (Remote File Checking)

A remote code execution vulnerability exists in the Microsoft Telnet service. An attacker who successfully exploited this vulnerability could 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: MS09-042  
<http://www.microsoft.com/technet/security/Bulletin/MS09-042.msp>
- \* BID: 35993  
<http://www.securityfocus.com/bid/35993>
- \* OSVDB: 56904  
<http://osvdb.org/56904>
- \* SECTRACK: 1022716  
<http://securitytracker.com/id?1022716>
- \* SECUNIA: 36222  
<http://secunia.com/advisories/36222>
- \* VUPEN: ADV-2009-2237  
<http://www.vupen.com/english/advisories/2009/2237>

## CVE Reference:

CVE-2009-1930 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

### • CVE-2009-2860 IBM CVSS 2.0 Score = 5.0

Unspecified vulnerability in db2jds in IBM DB2 8.1 before FP18 allows remote attackers to cause a denial of service (service crash) via "malicious packets."

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

## References:

- VUPEN: <http://www.vupen.com/english/advisories/2009/2293>
- CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg24024075>
- AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg11Z52433>
- SECUNIA: <http://secunia.com/advisories/36313>
- CONFIRM: [ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2\\_v82/APARLIST.TXT](ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2_v82/APARLIST.TXT)

**CVE Reference:** [CVE-2009-2860](#)

### • CVE-2009-2858 IBM CVSS 2.0 Score = 5.0

Memory leak in the Security component in IBM DB2 8.1 before FP18 on Unix platforms allows attackers to cause a denial of service (memory consumption) via unspecified vectors, related to private memory within the DB2 memory structure.

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

## References:

- CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg24024075>
- AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg11Z35635>
- SECUNIA: <http://secunia.com/advisories/36313>
- CONFIRM: [ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2\\_v82/APARLIST.TXT](ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2_v82/APARLIST.TXT)

**CVE Reference:** [CVE-2009-2858](#)

### • CVE-2009-2859 IBM CVSS 2.0 Score = 4.6

IBM DB2 8.1 before FP18 allows attackers to obtain unspecified access via a das command.

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

## References:

- VUPEN: <http://www.vupen.com/english/advisories/2009/2293>
- CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg24024075>

SECUNIA: <http://secunia.com/advisories/36313>

CONFIRM: [ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2\\_v82/APARLIST.TXT](ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2_v82/APARLIST.TXT)

**CVE Reference:** [CVE-2009-2859](#)

• **CVE-2008-7002 PHP CVSS 2.0 Score = 4.6**

PHP 5.2.5 does not enforce (a) open\_basedir and (b) safe\_mode\_exec\_dir restrictions for certain functions, which might allow local users to bypass intended access restrictions and call programs outside of the intended directory via the (1) exec, (2) system, (3) shell\_exec, (4) passthru, or (5) popen functions, possibly involving pathnames such as "C:" drive notation.

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

**References:**

BID: <http://www.securityfocus.com/bid/31064>

MISC: <http://downloads.securityfocus.com/vulnerabilities/exploits/31064.php>

**CVE Reference:** [CVE-2008-7002](#)

• **CVE-2009-2055 Cisco CVSS 2.0 Score = 4.3**

Cisco IOS XR 3.4.0 through 3.8.1 allows remote attackers to cause a denial of service (session reset) via a BGP UPDATE message with an invalid attribute, as demonstrated in the wild on 17 August 2009.

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

**References:**

CISCO: [http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af150f.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af150f.shtml)

SECTRAK: <http://securitytracker.com/id?1022739>

MLIST: <http://mailman.nanog.org/pipermail/nanog/2009-August/012719.html>

**CVE Reference:** [CVE-2009-2055](#)

• **CVE-2009-2846 Linux CVSS 2.0 Score = 7.8**

The eisa\_eeprom\_read function in the parisc isa-eeprom component (drivers/parisc/eisa\_eeprom.c) in the Linux kernel before 2.6.31-rc6 allows local users to access restricted memory via a negative ppos argument, which bypasses a check that assumes that ppos is positive and causes an out-of-bounds read in the readb function.

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

**References:**

MLIST: <http://www.openwall.com/lists/oss-security/2009/08/18/6>

MLIST: <http://www.openwall.com/lists/oss-security/2009/08/10/1>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=6b4dbcd86a9d464057fcc7abe4d0574093071f>

**CVE Reference:** [CVE-2009-2846](#)

• **CVE-2009-1878 Adobe CVSS 2.0 Score = 6.8**

Session fixation vulnerability in Adobe ColdFusion 8.0.1 and earlier allows remote attackers to hijack web sessions via unspecified vectors.

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

**References:**

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb09-12.html>

**CVE Reference:** [CVE-2009-1878](#)

• **CVE-2009-1876 Adobe CVSS 2.0 Score = 5.0**

Adobe ColdFusion 8.0.1 and earlier might allow attackers to obtain sensitive information via unspecified vectors, related to a "double-encoded null character vulnerability."

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

**References:**

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb09-12.html>

**CVE Reference:** [CVE-2009-1876](#)

**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)