

## 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

[Spida Digispid Worm Scanner](#) - The S4 Spida Digispid Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are prone any of the Microsoft Java Virtual Machine Vulnerabilities (MS02-069).

Download Here:

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

## This Week in Review

WPA encryption not enough anymore. SQL injection attack still alive. US court limits use of electronic evidence. US president wants power to shut down internet.

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

### • New attack cracks common Wi-Fi encryption in a minute

IDG News Service - Computer scientists in Japan say they've developed a way to break the WPA encryption system used in wireless routers in about one minute.

The attack gives hackers a way to read encrypted traffic sent between computers and certain types of routers that use the WPA (Wi-Fi Protected Access) encryption system. The attack was developed by Toshihiro Ohigashi of Hiroshima University and Masakatu Morii of Kobe University, who plan to discuss further details at a technical conference set for Sept. 25 in Hiroshima.

Last November, security researchers first showed how WPA could be broken, but the Japanese researchers have taken the attack to a new level, according to Dragos Ruiu, organizer of the PacSec security conference where the first WPA hack was demonstrated. "They took this stuff which was fairly theoretical and they've made it much more practical," he said. Computerworld

Full Story :

### • Mass SQL injection attacks still scaling up

The mass SQL injection attacks that gained attention earlier this week are continuing, with some 210,000 pages infected so far.

All of the attacks are coming from IP addresses based in China, Amichai Shulman, CTO of database security firm Imperva, told SCMagazineUS.com Thursday.

"This is something unique, as usually attacks of this nature come from infected bot PCs based all over the world rather than in one country," he said. "In this latest wave, we have recorded the attack coming from more than 60 servers based in China, attacking sites around the world, rather than the global network typically seen in such attacks." SC Magazine

Full Story :

<http://www.scmagazineus.com/Mass-SQL-injection-attacks-still-scaling-up/article/147490/>

### • Court ruling limits electronic searches

Computerworld - A federal appeals court this week ruled that government investigators cannot retain incriminating information found in electronic searches unless it is within the scope of a search warrant.

The U.S. Circuit Court of Appeals for the Ninth Circuit, in a 9-2 vote, rejected arguments by the U.S. Justice Department that it be allowed to retain and use all of the data that it seized in 2004 as part of a federal investigation into the use of illegal substances use by Major League Baseball players.

In a 63-page decision, the court disputed the Justice Department's argument that it should be allowed to retain and use information not included in its original search warrant because it came into "plain view." The court contended that the so-called "plain view doctrine," which allows investigators to seize evidence without a warrant if it was found in plain view during a legitimate search, does not extend to electronic searches. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9137209/Court\\_ruling\\_limits\\_electronic\\_searches?source=rss\\_security](http://www.computerworld.com/s/article/9137209/Court_ruling_limits_electronic_searches?source=rss_security)

### • Bill would give president emergency control of Internet

Internet companies and civil liberties groups were alarmed this spring when a U.S. Senate bill proposed handing the White House the power to disconnect private-sector computers from the Internet.

They're not much happier about a revised version that aides to Sen. Jay Rockefeller, a West Virginia Democrat, have spent months drafting behind closed doors. CNET News has obtained a copy of the 55-page draft (excerpt), which still appears to permit the president to seize temporary control of private-sector networks during a so-called cybersecurity emergency.

The new version would allow the president to "declare a cybersecurity emergency" relating to "non-governmental" computer networks and do what's necessary to respond to the threat. Other sections of the proposal include a federal certification program for "cybersecurity professionals," and a requirement that certain computer systems and networks in the private sector be managed by people who have been awarded that license. Cnet Security

Full Story :

[http://news.cnet.com/8301-13578\\_3-10320096-38.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-13578_3-10320096-38.html?part=rss&subj=news&tag=2547-1_3-0-20)

## New Vulnerabilities Tested in SecureScout

### • 13721 Oracle Database Server - Auditing component unspecified Vulnerability (jul-2009/CVE-2009-1969)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Auditing" component.

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

#### References:

\* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2009.html>

\* BID: 35689

<http://www.securityfocus.com/bid/35689>

\* OSVDB: 55894

<http://osvdb.org/55894>

\* SECTRACK: 1022560  
<http://www.securitytracker.com/id?1022560>  
\* SECUNIA: 35776  
<http://secunia.com/advisories/35776>  
\* VUPEN: ADV-2009-1900  
<http://www.vupen.com/english/advisories/2009/1900>

**CVE Reference:**

CVE-2009-1969 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **18483 Linux Kernel proto\_ops structures NULL pointer dereference Vulnerability**

The Linux kernel 2.6.0 through 2.6.30.4, and 2.4.4 through 2.4.37.4, does not initialize all function pointers for socket operations in proto\_ops structures, which allows local users to trigger a NULL pointer dereference and gain privileges by using mmap to map page zero, placing arbitrary code on this page, and then invoking an unavailable operation, as demonstrated by the sendpage operation (sock\_sendpage function) on a PF\_PPPOX socket.

The vulnerability is reported in versions prior to 2.4.37.5 and 2.6.31-rc6.

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

**References:**

\* BUGTRAQ: 20090813 Linux NULL pointer dereference due to incorrect proto\_ops initializations  
<http://www.securityfocus.com/archive/1/archive/1/505751/100/0/threaded>  
\* BUGTRAQ: 20090818 rPSA-2009-0121-1 kernel open-vm-tools  
<http://www.securityfocus.com/archive/1/archive/1/505912/100/0/threaded>  
\* FULLDISC: 20090813 Linux NULL pointer dereference due to incorrect proto\_ops initializations  
<http://archives.neohapsis.com/archives/fulldisclosure/2009-08/0174.html>  
\* MILWORM: 9477  
<http://www.milw0rm.com/exploits/9477>  
\* MISC:  
<http://blog.cr0.org/2009/08/linux-null-pointer-dereference-due-to.html>  
\* MISC:  
[http://grsecurity.net/~spender/wunderbar\\_emporium.tgz](http://grsecurity.net/~spender/wunderbar_emporium.tgz)  
\* MISC:  
<http://zenthought.org/content/file/android-root-2009-08-16-source>  
\* CONFIRM:  
<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=e694958388c50148389b0e9b9e9e8945cf0f1b98>  
\* CONFIRM:  
<http://www.kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.37.5>  
\* CONFIRM:  
<http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.31-rc6>  
\* CONFIRM:  
<http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.30.5>  
\* CONFIRM:  
<http://wiki.rpath.com/wiki/Advisories:rPSA-2009-0121>  
\* CONFIRM:  
<https://issues.rpath.com/browse/RPL-3103>  
\* DEBIAN: DSA-1865  
<http://www.debian.org/security/2009/dsa-1865>  
\* BID: 36038  
<http://www.securityfocus.com/bid/36038>  
\* SECUNIA: 36289  
<http://secunia.com/advisories/36289>  
\* SECUNIA: 36327  
<http://secunia.com/advisories/36327>  
\* VUPEN: ADV-2009-2272  
<http://www.vupen.com/english/advisories/2009/2272>

**CVE Reference:**

CVE-2009-2692 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **18484 Oracle Application Server - Oracle Security Developer Tools component unspecified Vulnerability (jul-2009/CVE-2009-0217)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Oracle Security Developer Tools" component.

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

## References:

\* MISC:

[http://www.w3.org/QA/2009/07/hmac\\_truncation\\_in\\_xml\\_signatu.html](http://www.w3.org/QA/2009/07/hmac_truncation_in_xml_signatu.html)

\* CONFIRM:

<http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg21384925>

\* CONFIRM:

<http://www.aleksey.com/xmlsec/>

\* CONFIRM:

<http://www.mono-project.com/Vulnerabilities>

\* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2009.html>

\* CONFIRM:

<http://www.w3.org/2008/06/xmlsigcore-errata.html#e03>

\* CONFIRM:

[https://issues.apache.org/bugzilla/show\\_bug.cgi?id=47527](https://issues.apache.org/bugzilla/show_bug.cgi?id=47527)

\* CONFIRM:

<http://www.kb.cert.org/vuls/id/MAPG-7TSKXQ>

\* CONFIRM:

<http://sunsolve.sun.com/search/document.do?assetkey=1-21-125136-16-1>

\* CONFIRM:

[http://blogs.sun.com/security/entry/cert\\_vulnerability\\_note\\_vu\\_466161](http://blogs.sun.com/security/entry/cert_vulnerability_note_vu_466161)

\* CONFIRM:

<http://www.kb.cert.org/vuls/id/WDON-7TY529>

\* CONFIRM:

[https://issues.apache.org/bugzilla/show\\_bug.cgi?id=47526](https://issues.apache.org/bugzilla/show_bug.cgi?id=47526)

\* AIXAPAR: PK80596

<http://www-01.ibm.com/support/docview.wss?rs=180&context=SSEQTP&dc=D400&uid=swg24023545&am>

\* AIXAPAR: PK80627

<http://www-01.ibm.com/support/docview.wss?rs=180&context=SSEQTP&dc=D400&uid=swg24023723&am>

\* FEDORA: FEDORA-2009-8329

<https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html>

\* FEDORA: FEDORA-2009-8337

<https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html>

\* FEDORA: FEDORA-2009-8456

<https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00494.html>

\* FEDORA: FEDORA-2009-8473

<https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00505.html>

\* MANDRIVA: MDVSA-2009:209

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:209>

\* REDHAT: RHSA-2009:1200

<https://rhn.redhat.com/errata/RHSA-2009-1200.html>

\* REDHAT: RHSA-2009:1201

<https://rhn.redhat.com/errata/RHSA-2009-1201.html>

\* SUNALERT: 263429

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-263429-1>

\* CERT-VN: VU#466161

<http://www.kb.cert.org/vuls/id/466161>

\* BID: 35671

<http://www.securityfocus.com/bid/35671>

\* OSVDB: 55895

<http://osvdb.org/55895>

\* OSVDB: 55907

<http://osvdb.org/55907>

\* SECTRACK: 1022561

<http://www.securitytracker.com/id?1022561>

\* SECTRACK: 1022567

<http://www.securitytracker.com/id?1022567>

\* SECTRACK: 1022661

<http://www.securitytracker.com/id?1022661>

\* SECUNIA: 35776

<http://secunia.com/advisories/35776>

\* SECUNIA: 35853

<http://secunia.com/advisories/35853>

\* SECUNIA: 35854

<http://secunia.com/advisories/35854>

\* SECUNIA: 35855

<http://secunia.com/advisories/35855>

\* SECUNIA: 35858

<http://secunia.com/advisories/35858>

\* SECUNIA: 36162  
<http://secunia.com/advisories/36162>  
\* SECUNIA: 36176  
<http://secunia.com/advisories/36176>  
\* SECUNIA: 36180  
<http://secunia.com/advisories/36180>  
\* SECUNIA: 35852  
<http://secunia.com/advisories/35852>  
\* VUPEN: ADV-2009-1900  
<http://www.vupen.com/english/advisories/2009/1900>  
\* VUPEN: ADV-2009-1908  
<http://www.vupen.com/english/advisories/2009/1908>  
\* VUPEN: ADV-2009-1911  
<http://www.vupen.com/english/advisories/2009/1911>  
\* VUPEN: ADV-2009-1909  
<http://www.vupen.com/english/advisories/2009/1909>

#### CVE Reference:

CVE-2009-0217 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18485 Oracle Application Server - HTTP Server component unspecified Vulnerability (jul-2009/CVE-2009-1976)

An unspecified vulnerability with unknown impact exists in Oracle Application Server "HTTP Server" component.

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

#### References:

\* CONFIRM:  
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpupjul2009.html>  
\* BID: 35688  
<http://www.securityfocus.com/bid/35688>  
\* OSVDB: 55896  
<http://osvdb.org/55896>  
\* SECTRACK: 1022567  
<http://www.securitytracker.com/id?1022567>  
\* SECUNIA: 35776  
<http://secunia.com/advisories/35776>  
\* VUPEN: ADV-2009-1900  
<http://www.vupen.com/english/advisories/2009/1900>  
\* XF: oracle-as-httpserver-unspecified(51760)  
<http://xforce.iss.net/xforce/xfdb/51760>

#### CVE Reference:

CVE-2009-1976 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18486 Cisco IOS Software Mobile IP and Mobile IPv6 Vulnerabilities (cisco-sa-20090325-mobileip) (CVE-2009-0634)

Multiple unspecified vulnerabilities in the home agent (HA) implementation in the (1) Mobile IP NAT Traversal feature and (2) Mobile IPv6 subsystem in Cisco IOS 12.3 through 12.4 allow remote attackers to cause a denial of service (input queue wedge and interface outage) via an ICMP packet.

This vulnerability is documented in Cisco bug ID CSCso05337.

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

#### References:

\* CONFIRM:  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080a90469.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080a90469.shtml)  
\* CISCO: 20090325 Cisco IOS Software Mobile IP and Mobile IPv6 Vulnerabilities  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080a9042f.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080a9042f.shtml)  
\* BID: 34241  
<http://www.securityfocus.com/bid/34241>  
\* SECTRACK: 1021898  
<http://securitytracker.com/id?1021898>  
\* SECUNIA: 34438  
<http://secunia.com/advisories/34438>  
\* VUPEN: ADV-2009-0851

<http://www.vupen.com/english/advisories/2009/0851>

\* XF: ios-mobile-dos(49424)

<http://xforce.iss.net/xforce/xfdb/49424>

\* XF: ios-mobile-ha-dos(49585)

<http://xforce.iss.net/xforce/xfdb/49585>

**CVE Reference:**

CVE-2009-0634 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18487 Cisco IOS Software Mobile IP and Mobile IPv6 Vulnerabilities (cisco-sa-20090325-mobileip) (CVE-2009-0633)**

Multiple unspecified vulnerabilities in the (1) Mobile IP NAT Traversal feature and (2) Mobile IPv6 subsystem in Cisco IOS 12.3 through 12.4 allow remote attackers to cause a denial of service (input queue wedge and interface outage) via MIPv6 packets.

This vulnerability is documented in Cisco bug ID CSCsm97220.

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

**References:**

\* CONFIRM:

[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080a90469.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080a90469.shtml)

\* CISCO: 20090325 Cisco IOS Software Mobile IP and Mobile IPv6 Vulnerabilities

[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080a9042f.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080a9042f.shtml)

\* BID: 34241

<http://www.securityfocus.com/bid/34241>

\* SECTrack: 1021898

<http://securitytracker.com/id?1021898>

\* SECUNIA: 34438

<http://secunia.com/advisories/34438>

\* VUPEN: ADV-2009-0851

<http://www.vupen.com/english/advisories/2009/0851>

\* XF: ios-mobile-dos(49424)

<http://xforce.iss.net/xforce/xfdb/49424>

**CVE Reference:**

CVE-2009-0633 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18488 Cisco IOS Software Multiple Features IP Sockets Vulnerability (cisco-sa-20090325-ip)**

The (1) Cisco Unified Communications Manager Express; (2) SIP Gateway Signaling Support Over Transport Layer Security (TLS) Transport; (3) Secure Signaling and Media Encryption; (4) Blocks Extensible Exchange Protocol (BEEP); (5) Network Admission Control HTTP Authentication Proxy; (6) Per-user URL Redirect for EAPoUDP, Dot1x, and MAC Authentication Bypass; (7) Distributed Director with HTTP Redirects; and (8) TCP DNS features in Cisco IOS 12.0 through 12.4 do not properly handle IP sockets, which allows remote attackers to cause a denial of service (outage or resource consumption) via a series of crafted TCP packets.

This vulnerability is documented in Cisco bug ID CSCsm27071.

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

**References:**

\* CONFIRM:

[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080a90469.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080a90469.shtml)

\* CISCO: 20090325 Cisco IOS Software Multiple Features IP Sockets Vulnerability

[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080a904c6.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080a904c6.shtml)

\* BID: 34242

<http://www.securityfocus.com/bid/34242>

\* SECTrack: 1021897

<http://securitytracker.com/id?1021897>

\* SECUNIA: 34438

<http://secunia.com/advisories/34438>

\* VUPEN: ADV-2009-0851

<http://www.vupen.com/english/advisories/2009/0851>

\* XF: ios-ipsockets-dos(49418)

<http://xforce.iss.net/xforce/xfdb/49418>

**CVE Reference:**

CVE-2009-0630 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18489 Cisco IOS cTCP Denial of Service Vulnerability (cisco-sa-20090325-ctcp)**

The Cisco Tunneling Control Protocol (cTCP) feature is used by Easy VPN remote device operating in an environment in which standard IPSec does not function transparently without modification to existing firewall rules. The cTCP traffic is actually TCP traffic. Cisco IOS cTCP packets are Internet Key Exchange (IKE) or Encapsulating Security Payload (ESP) packets that are being transmitted over TCP.

A vulnerability exists where a series of TCP packets may cause a Cisco IOS device that is configured as an Easy VPN server with the cTCP encapsulation feature to run out of memory.

This vulnerability is documented in Cisco Bug IDs CSCsr16693 and CSCsu21828.

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

**References:**

\* CONFIRM:

[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080a90469.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080a90469.shtml)

\* CISCO: 20090325 Cisco IOS cTCP Denial of Service Vulnerability

[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080a90459.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080a90459.shtml)

\* BID: 34246

<http://www.securityfocus.com/bid/34246>

\* SECTRAK: 1021895

<http://www.securitytracker.com/id?1021895>

\* SECUNIA: 34438

<http://secunia.com/advisories/34438>

\* VUPEN: ADV-2009-0851

<http://www.vupen.com/english/advisories/2009/0851>

\* XF: ios-ctcp-dos(49417)

<http://xforce.iss.net/xforce/xfdb/49417>

**CVE Reference:**

CVE-2009-0635 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18490 Cisco IOS Software Secure Copy Privilege Escalation Vulnerability (cisco-sa-20090325-scp)**

SCP is a protocol similar to the Remote Copy (RCP) protocol, which allows the transfer of files between systems. The main difference between SCP and RCP is that in SCP, all aspects of the file transfer session, including authentication, occur in encrypted form, which makes SCP a more secure alternative than RCP. SCP relies on the Secure Shell (SSH) protocol, which uses TCP port 22 by default.

The Role-Based CLI Access feature allows the network administrator to define "views". Views are sets of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS software EXEC and configuration (Config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. For more information about the Role-Based CLI Access feature, reference [http://www.cisco.com/en/US/docs/ios/12\\_3t/12\\_3t7/feature/guide/gtclivws.html](http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtclivws.html).

The server side of the SCP implementation in Cisco IOS software contains a vulnerability that allows authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be a SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow authenticated users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files. This configuration file may include passwords or other sensitive information.

In the affected configuration presented in the Affected Products section, users confined to a CLI view can elevate their privileges by using SCP to write to the device's configuration. Note that a view can be attached to a user when defining the user in the local database (via the username <user name> view ... command), or by passing the attribute cli-view-name from an AAA server.

This vulnerability does not allow for authentication bypass; login credentials are verified and access is only granted if a valid username and password is provided. This vulnerability may cause authorization to be bypassed.

This vulnerability is documented in the Cisco Bug ID CSCsv38166.

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

**References:**

\* CONFIRM:

[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080a90469.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080a90469.shtml)

\* CISCO: 20090325 Cisco IOS Software Secure Copy Privilege Escalation Vulnerability

[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080a904c8.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080a904c8.shtml)

\* BID: 34247

<http://www.securityfocus.com/bid/34247>

\* SECTRAK: 1021899

<http://securitytracker.com/id?1021899>

\* SECUNIA: 34438

<http://secunia.com/advisories/34438>

\* VUPEN: ADV-2009-0851

<http://www.vupen.com/english/advisories/2009/0851>

\* XF: ios-scp-priv-escalation(49423)

<http://xforce.iss.net/xforce/xfdb/49423>

#### CVE Reference:

CVE-2009-0637 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18491 Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability (cisco-sa-20090325-sip)

SIP is a popular signaling protocol that is used to manage voice and video calls across IP networks such as the Internet. SIP is responsible for handling all aspects of call setup and termination. Voice and video are the most popular types of sessions that SIP handles, but the protocol has the flexibility to accommodate other applications that require call setup and termination. SIP call signaling can use UDP (port 5060), TCP (port 5060), or TLS (TCP port 5061) as the underlying transport protocol.

A denial of service (DoS) vulnerability exists in the SIP implementation in Cisco IOS Software. This vulnerability is triggered by processing a specific and valid SIP message.

This vulnerability is documented in Cisco Bug ID CSCsu11522.

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

#### References:

\* CONFIRM:

[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080a90469.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080a90469.shtml)

\* CISCO: 20090325 Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability

[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080a904c0.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080a904c0.shtml)

\* BID: 34243

<http://www.securityfocus.com/bid/34243>

\* SECTRAK: 1021902

<http://securitytracker.com/id?1021902>

\* SECUNIA: 34438

<http://secunia.com/advisories/34438>

\* VUPEN: ADV-2009-0851

<http://www.vupen.com/english/advisories/2009/0851>

\* XF: ios-sip-dos(49421)

<http://xforce.iss.net/xforce/xfdb/49421>

#### CVE Reference:

CVE-2009-0636 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

#### • CVE-2009-2954 Microsoft CVSS 2.0 Score = 5.0

Microsoft Internet Explorer 6.0.2900.2180 and earlier allows remote attackers to cause a denial of service (CPU consumption and application hang) via JavaScript code with a long string value for the hash property (aka location.hash), a related issue to CVE-2008-5715.

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

#### References:

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/506006/100/0/threaded>

MISC: <http://websecurity.com.ua/3424/>

**CVE Reference:** [CVE-2009-2954](#)

• **CVE-2009-2956 IBM CVSS 2.0 Score = 5.0**

The (1) Net.Commerce and (2) Net.Data components in IBM WebSphere Commerce Suite store sensitive information under the web root with insufficient access control, which allows remote attackers to discover passwords, and database and filesystem details, via direct requests for configuration files.

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

**References:**

XF: <http://xforce.iss.net/xforce/xfdb/52616>

**CVE Reference:** [CVE-2009-2956](#)

• **CVE-2009-2054 Cisco CVSS 2.0 Score = 7.8**

Cisco Unified Communications Manager (aka CUCM, formerly CallManager) 4.x, 5.x before 5.1(3g), 6.x before 6.1(4), 7.0 before 7.0(2a)su1, and 7.1 before 7.1(2a)su1 allows remote attackers to cause a denial of service (file-descriptor exhaustion and SIP outage) via a flood of TCP packets, aka Bug ID CSCsx23689.

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

**References:**

CISCO: [http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af2d11.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af2d11.shtml)

BID: <http://www.securityfocus.com/bid/36152>

**CVE Reference:** [CVE-2009-2054](#)

• **CVE-2009-2053 Cisco CVSS 2.0 Score = 7.8**

Cisco Unified Communications Manager (aka CUCM, formerly CallManager) 4.x, 5.x before 5.1(3g), 6.x before 6.1(4), 7.0 before 7.0(2a)su1, and 7.1 before 7.1(2) allows remote attackers to cause a denial of service (file-descriptor exhaustion and SCCP outage) via a flood of TCP packets, aka Bug ID CSCsx32236.

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

**References:**

CISCO: [http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af2d11.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af2d11.shtml)

BID: <http://www.securityfocus.com/bid/36152>

**CVE Reference:** [CVE-2009-2053](#)

• **CVE-2009-2051 Cisco CVSS 2.0 Score = 7.8**

Cisco Unified Communications Manager (aka CUCM, formerly CallManager) 4.x, 5.x before 5.1(3g), 6.x before 6.1(4), and 7.x before 7.1(2) allows remote attackers to cause a denial of service (voice-services outage) via a malformed SIP INVITE message that triggers an improper call to the sipSafeStrlen function, aka Bug ID CSCsz40392.

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

**References:**

CISCO: [http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af2d11.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af2d11.shtml)

BID: <http://www.securityfocus.com/bid/36152>

**CVE Reference:** [CVE-2009-2051](#)

• **CVE-2009-2052 Cisco CVSS 2.0 Score = 7.8**

Cisco Unified Communications Manager (aka CUCM, formerly CallManager) 4.x, 5.x before 5.1(3g), 6.x before 6.1(4), 7.0 before 7.0(2), and 7.1 before 7.1(2) allows remote attackers to cause a denial of service (TCP services outage) via a large number of TCP connections, related to "tracking of network connections," aka Bug ID CSCsq22534.

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

**References:**

CISCO: [http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af2d11.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af2d11.shtml)

BID: <http://www.securityfocus.com/bid/36152>

**CVE Reference:** [CVE-2009-2052](#)

• **CVE-2009-2050 Cisco CVSS 2.0 Score = 7.8**

Cisco Unified Communications Manager (aka CUCM, formerly CallManager) before 6.1(1) allows remote attackers to cause a denial of service (voice-services outage) via a malformed header in a SIP message, aka Bug ID CSCsi46466.

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

**References:**

CISCO: [http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af2d11.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af2d11.shtml)

BID: <http://www.securityfocus.com/bid/36152>

**CVE Reference:** [CVE-2009-2050](#)

• **CVE-2009-2861 Cisco CVSS 2.0 Score = 7.3**

The Over-the-Air Provisioning (OTAP) functionality on Cisco Aironet Lightweight Access Point 1100 and 1200 devices does not properly implement access-point association, which allows remote attackers to spoof a controller and cause a denial of service (service outage) via crafted remote radio management (RRM) packets, aka "SkyJack" or Bug ID CSCtb56664.

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

**References:**

CONFIRM: <http://tools.cisco.com/security/center/viewAlert.x?alertId=18919>

VUPEN: <http://www.vupen.com/english/advisories/2009/2419>

BID: <http://www.securityfocus.com/bid/36145>

MISC: [http://www.airmagnet.com/news/press\\_releases/2009/08252009.php](http://www.airmagnet.com/news/press_releases/2009/08252009.php)

MISC: [http://www.airmagnet.com/assets/AM\\_Technote\\_SkyJack\\_082509.pdf](http://www.airmagnet.com/assets/AM_Technote_SkyJack_082509.pdf)

SECTRAK: <http://securitytracker.com/id?1022774>

**CVE Reference:** [CVE-2009-2861](#)

## **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)