

[Solutions](#) | [Products](#) | [Ordering](#) | [Support](#) | [Partners](#) | [Training](#) | [Corporate](#)[Security Advisories](#)

# Cisco Security Advisory: Vulnerabilities in Cisco Video Surveillance Products

Advisory ID: [cisco-sa-20090624-video](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20090624-video.shtml>

## Revision 1.0

For Public Release 2009 June 24 1600 UTC (GMT)

---

Please provide your [feedback](#) on this document.

---

## Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Vulnerability Scoring Details](#)
- [Impact](#)
- [Software Versions and Fixes](#)
- [Workarounds](#)
- [Obtaining Fixed Software](#)
- [Exploitation and Public Announcements](#)
- [Status of this Notice: FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

---

## Summary

Cisco Video Surveillance Stream Manager firmware for the Cisco Video Surveillance Services Platforms and Cisco Video Surveillance Integrated Services Platforms contain a denial of service (DoS) vulnerability that could result in a reboot on systems that receive a crafted packet.

Cisco Video Surveillance 2500 Series IP Cameras contain an information disclosure vulnerability that could allow an authenticated user to view any file on a vulnerable camera.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds that mitigate these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090624-video.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

## ☐ **Affected Products**

### ☐ **Vulnerable Products**

The following products are vulnerable:

- Cisco Video Surveillance Stream Manager firmware for the Cisco Video Surveillance Services Platform versions prior to 5.3
- Cisco Video Surveillance Stream Manager firmware for the Cisco Video Surveillance Integrated Services Platform versions prior to 5.3
- Cisco Video Surveillance 2500 Series IP Camera firmware versions prior to 2.1

### ☐ **Products Confirmed Not Vulnerable**

No other Cisco products are currently known to be affected by these vulnerabilities.

[Top of the section](#) [Close Section](#)

## ☐ **Details**

Cisco Video Surveillance Services Platforms and Cisco Video Surveillance Integrated Services Platforms are vulnerable to a DoS condition. An attacker could exploit this vulnerability by sending a crafted packet to UDP port 37000, which could cause the crash of a critical process and result in a system reboot. This vulnerability is documented in Cisco Bug ID CSCsj47924 and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2009-2045.

Cisco Video Surveillance 2500 Series IP Cameras contain an information disclosure vulnerability. An authenticated user may be able to access a vulnerable camera and view any file through the embedded web server on TCP ports 80 (HTTP) and/or 443 (HTTPS), depending on the camera configuration. This vulnerability is documented in Cisco Bug IDs CSCsu05515 and CSCsr96497 (Wireless Cameras) and has been assigned Common Vulnerabilities and Exposures

(CVE) identifier CVE-2009-2046.

[Top of the section](#)   [Close Section](#)

## ▣ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at:

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at:

<http://intellishield.cisco.com/security/alertmanager/cvss>

<b><a href="#">CSCsj47924 - Malformed payload to xvrman process causes reboot</a></b> ( <a href="#">registered</a> customers only)					
<b>Calculate the environmental score of <a href="#">CSCsj47924</a></b>					
CVSS Base Score - <b>7.8</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - <b>6.4</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

<b><a href="#">CSCsu05515 - SD Camera Web Server Will Display any File on System</a></b> ( <a href="#">registered</a> customers only)					
<b>Calculate the environmental score of <a href="#">CSCsu05515</a></b>					
CVSS Base Score - <b>6.8</b>					

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Complete	None	None
CVSS Temporal Score - <b>5.6</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

<a href="#">CSCsr96497 - Wireless Camera HTTP Server Will Display any File on System</a> ( <a href="#">registered</a> customers only)					
<b>Calculate the environmental score of <a href="#">CSCsr96497</a></b>					
CVSS Base Score - <b>6.8</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Complete	None	None
CVSS Temporal Score - <b>5.6</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

[Top of the section](#)   [Close Section](#)

## ☐ Impact

Successful exploitation of the Cisco Video Surveillance Stream Manager firmware vulnerability could cause a system reboot. Repeated exploitation may result in an extended DoS condition, which could prevent administrators from viewing video surveillance feeds.

Successful exploitation of the Cisco Video Surveillance 2500 Series IP Cameras vulnerability could allow an authenticated user to view any file on a vulnerable camera. This vulnerability could allow a non-privileged user to obtain privileged access.

[Top of the section](#)   [Close Section](#)

## ☐ Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

Cisco Video Surveillance Stream Manager firmware for the Cisco Video Surveillance Services Platform version 5.3 is available for download here:

<http://tools.cisco.com/support/downloads/go/ReleaseType.x?optPlat=Linux&isPlatform=Y&mdfid=281158836&sftType=Video+Surveillance+S>

Cisco Video Surveillance Stream Manager firmware for the Cisco Video Surveillance Integrated Services Platform version 5.3 is available for download here:

<http://tools.cisco.com/support/downloads/go/ReleaseType.x?optPlat=Linux&isPlatform=Y&mdfid=281158834&sftType=Video+Surveillance+S>

Cisco Video Surveillance 2500 Series IP Camera firmware version 2.1 is available for download here:

<http://tools.cisco.com/support/downloads/go/ReleaseType.x?optPlat=Linux&isPlatform=Y&mdfid=282052803&sftType=Video+Surveillance+I>

[Top of the section](#)   [Close Section](#)

## ☐ Workarounds

Although there are no workarounds for these vulnerabilities, it is possible to mitigate the vulnerabilities through the use of network filters. Administrators are advised to restrict access to UDP port 37000 on vulnerable Cisco Video Surveillance Services Platform and Integrated Services Platform systems to trusted hosts. On Cisco Video Surveillance 2500 Series IP Cameras, administrators are advised to restrict access to TCP ports 80 and 443 to trusted hosts.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory, which is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-amb-20090624-video.shtml>

[Top of the section](#)   [Close Section](#)

## ☐ Obtaining Fixed Software

Cisco has released free software updates that address these vulnerabilities. Prior to

deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing, or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at

[http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN\\_.html](http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html), or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact [psirt@cisco.com](mailto:psirt@cisco.com) or [security-alert@cisco.com](mailto:security-alert@cisco.com) for software upgrades.

### ☐ **Customers with Service Contracts**

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

### ☐ **Customers using Third Party Support Organizations**

Customers whose Cisco products are provided or maintained through prior or existing agreements with third-party support organizations, such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations, such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

### ☐ **Customers without Service Contracts**

Customers who purchase direct from Cisco but do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)

- e-mail: [tac@cisco.com](mailto:tac@cisco.com)

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to

[http://www.cisco.com/en/US/support/tsd\\_cisco\\_worldwide\\_contacts.html](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html) for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

[Top of the section](#)   [Close Section](#)

## ☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

These vulnerabilities were discovered by Cisco.

[Top of the section](#)   [Close Section](#)

## ☐ **Status of this Notice: FINAL**

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

[Top of the section](#)   [Close Section](#)

## ☐ **Distribution**

This advisory is posted on Cisco's worldwide website at :

<http://www.cisco.com/warp/public/707/cisco-sa-20090624-video.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- [cust-security-announce@cisco.com](mailto:cust-security-announce@cisco.com)
- [first-bulletins@lists.first.org](mailto:first-bulletins@lists.first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto:comp.dcom.sys.cisco@newsgate.cisco.com)

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

[Top of the section](#)   [Close Section](#)

## ☐ Revision History

Revision 1.0	2009-June- 24	Initial public release
-----------------	------------------	---------------------------

[Top of the section](#)   [Close Section](#)

## ☐ Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

[Top of the section](#)   [Close Section](#)

---

### Help us help you.

☐ Please rate this document.

- Excellent  
 Good  
 Average  
 Fair  
 Poor

**This document solved my problem.**

- Yes  
 No  
 Just browsing

**Suggestions for improvement:**

(256 character limit)

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)