

Cisco Security Advisory: Cisco Video Surveillance IP Gateway and Services Platform Authentication Vulnerabilities

Advisory ID: [cisco-sa-20070905-video](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20070905-video.shtml>

Revision 1.0

For Public Release 2007 September 5 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 IP Gateway video encoder and decoder, Services Platform (SP), and Integrated Services Platform (ISP) devices contain authentication vulnerabilities that allow remote users with network connectivity to gain the complete administrative control of vulnerable devices. There are no workarounds for these vulnerabilities.

Cisco has made free software available to address these vulnerabilities for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070905-video.shtml>.

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

☐ **Affected Products**

☐ **Vulnerable Products**

These products are vulnerable:

- Cisco Video Surveillance IP Gateway Encoder/Decoder (Standalone and Module) firmware version 1.8.1 and earlier
- Cisco Video Surveillance SP/ISP Decoder Software firmware version 1.11.0 and earlier
- Cisco Video Surveillance SP/ISP firmware version 1.23.7 and earlier

Users should consult their Stream Manager configuration management tool to determine the versions of firmware installed on deployed video surveillance devices.

☐ **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 IP Gateway video encoders and decoders allow the video feeds of cameras to be sent over an IP network. This function provides an upgrade path for users to convert from existing analog surveillance systems. Cisco Video Surveillance Services Platforms and Integrated Services Platforms record and aggregate video feeds received from IP Gateways. Stored video can be viewed and manipulated using the Cisco Video Surveillance Stream Manager software.

- **IP Gateway Encoder/Decoder Telnet Authentication Vulnerability:**
The Telnet server installed on Cisco Video Surveillance IP Gateway video encoders and decoders does not prompt for authentication. This may allow a remote user with network connectivity to gain interactive shell access with administrative privileges on vulnerable devices. This issue is documented in Cisco Bug ID [CSCsj31729](#) ([registered](#) customers only) .
- **Services Platform/Integrated Services Platform Default Authentication Vulnerability:**
Cisco Video Surveillance Services Platform and Integrated Services Platform devices ship with default passwords for the sytix and root user accounts. Users are not able to change these passwords due to application requirements. Users with knowledge of the default passwords may be able to gain interactive shell access with administrative privileges to vulnerable devices. This issue is documented in Cisco Bug ID [CSCsj34681](#) ([registered](#) customers only) .

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

▣ Vulnerability Scoring Details

Cisco is providing 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.

Cisco will provide a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerabilities in individual networks.

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

Cisco has provided a 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>.

CSCsj31729 - Encoder / Decoder Telnet Daemon Fails to Authenticate (registered customers only)					
Calculate the environmental score of CSCsj31729					
CVSS Base Score - 10					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - 8.7					
Exploitability		Remediation Level		Report Confidence	
High		Official-Fix		Confirmed	

CSCsj34681 - Services Platform Contains Default Authentication Credentials (registered customers only)					
Calculate the environmental score of CSCsj34681					
CVSS Base Score - 9.0					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Complete	Complete	Complete
CVSS Temporal Score - 7.8					
Exploitability		Remediation Level		Report Confidence	

High

Official-Fix

Confirmed

[Top of the section](#)

[Close Section](#)

☐ Impact

Successful exploitation of these vulnerabilities will result in the ability for a remote user to gain complete administrative access to vulnerable devices. An attacker with access to a vulnerable device may be able to view, alter, or delete video streams processed by the device, or cause a denial of service that may result in the loss of surveillance coverage.

[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.

[Top of the section](#)

[Close Section](#)

☐ Workarounds

There are no workarounds for these vulnerabilities.

Filtering traffic to affected systems on screening devices can be used as a mitigation technique for both vulnerabilities. Access to the Telnet service (TCP port 23) on vulnerable devices should be restricted to authorized administration workstations.

There is currently no method to configure filtering directly on IP Gateway encoders and decoders or Services Platform devices.

Filters blocking access to TCP port 23 should be deployed at the network edge as part of a transit access list, which will protect the router where the access control list (ACL) is configured and also other devices behind it. Further information about transit access control lists is available in the white paper *Transit Access Control Lists: Filtering at Your Edge*, which is available at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml

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:

<http://www.cisco.com/warp/public/707/cisco-amb-20070905-video.shtml>

❏ **Obtaining Fixed Software**

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/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Customers with vulnerable devices should contact the Cisco TAC or their primary support organization to obtain fixed software and upgrade instructions.

Device	Vulnerable Firmware	Fixed Firmware
Cisco Video Surveillance IP Gateway Encoder/Decoder	1.8.1 and earlier	1.9.4
Cisco Video Surveillance SP/ISP Decoder Software	1.11.0 and earlier	1.16.0
Cisco Video Surveillance SP/ISP	1.23.7 and earlier	1.26.0

❏ **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 agreement 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 who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their 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

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

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special 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 internally 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-20070905-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
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- 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	2007-Sept-05	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. 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)

Send

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).