



Release Notes for Cisco Video Surveillance High Definition IP Camera Release 3.2.4

First Published: May 2014

These release notes provide important information for the Cisco Video Surveillance high definition IP camera release 3.2.4.

Firmware release 3.2.4 applies to the following Cisco IP camera models:

- CIVS-IPC-4300E
- CIVS-IPC-4500E

This firmware is compatible with Cisco Video Surveillance Manager (VSM) 6.3.2 and VSM 7.2 with Driver Pack dp_cisco-2.0-32d_7.2.0-020d. For information about upgrading the IP camera through VSM, refer to the *Release Notes for Cisco Video Surveillance Manager* at:

http://www.cisco.com/en/US/partner/products/ps10818/prod_release_notes_list.html

Contents

This document includes the following sections:

- [What's New in this Release, page 2](#)
- [Upgrading to Release 3.2.4, page 2](#)
- [Using the Upgrade Hot Fix Utility to Upgrade from Release 3.1.0 to Release 3.1.1, page 3](#)
- [Limitations and Restrictions, page 4](#)
- [Caveats, page 5](#)
- [Related Documentation, page 6](#)
- [Obtaining Documentation and Submitting a Service Request, page 6](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

What's New in this Release

Cisco Video Surveillance IP camera firmware release 3.2.4 resolves CSCuo37283, the camera vulnerability to CVE-2014-0160- Heartbleed. Cisco recommends that you upgrade to this latest release.

For more information, see the “Caveats” section on page 5.

Upgrading to Release 3.2.4



Caution

Do not use the procedure in this section to upgrade your IP camera to Release 3.2.4 if the IP camera part number is 74-9125-02 or 74-9126-02 and firmware release is 3.1.0. Instead, you must use an upgrade hot fix utility available on Cisco.com to upgrade from Release 3.1.0 to Release 3.1.1. You can then use the procedure in this section to upgrade from Release 3.1.1 to Release 3.2.1. For more information about upgrading your IP camera using an upgrade hot fix utility, see the “Using the Upgrade Hot Fix Utility to Upgrade from Release 3.1.0 to Release 3.1.1” section on page 3.

If your IP camera part number is not 74-9125-02 or 74-9126-02, you can use the procedure in this section to upgrade to Release 3.2.4. You can find the IP camera part number listed on the camera user interface Home window, under the General Information area.

You can upgrade your IP camera to firmware 3.2.4 by using the Camera Firmware Upgrade feature in the VSM Management Console. For instructions, see the “Using the VSM Management Console” chapter in *Cisco Video Surveillance Manager User Guide*.

Alternatively, you can upgrade your IP camera to release 3.2.4 by performing the following steps.

Procedure

- Step 1** Take these actions to obtain the release 3.2.4 firmware:
- a. Go to this URL:
<http://www.cisco.com/cisco/software/release.html?mdfid=282582478&flowid=31387&softwareid=282090156&os=Linux&release=3.2.2>
 - b. Download the 3.2.4 firmware file named **CVIS-IPC-4xxxE-V3.2.4-223.bin**.
 - c. Log in and follow the on-screen prompts to download it to your PC.
- Step 2** Take these actions to display the Firmware window in the web interface for your IP camera:
- a. Start Internet Explorer and enter the following in the address field:
`protocol://ip_address:port_number`
 where:
 - *protocol* is the connection that you use for your IP camera (either HTTPS or HTTP).
 - *ip_address* is the IP address of your IP camera.
 - *port_number* is the port number that is used for HTTPS or HTTP connections to the IP camera. You do not need to enter a port number if you are connecting through the default HTTPS port 443 or the default HTTP port 80.
 - b. Enter your IP camera user name and password when prompted, then click **OK**.

The IP Camera Main window appears.

- c. Click the **Setup** link to access configuration menus for the camera.
- d. Click **Administration**, then click **Firmware**.

The Firmware Settings window appears.

Step 3 In the Firmware window, click the **Upgrade** button.

The Upgrade Firmware window appears.

Step 4 In the Upgrade Firmware window, click the **Browse** button, choose the upgrade file, and then click **Open**.

The upgrade file may be stored on another PC.

Step 5 Click **Upgrade**.

Do not power down the IP camera during the upgrade procedure.

After you upgrade the firmware, the IP camera automatically restarts. It retains all configuration information.

Using the Upgrade Hot Fix Utility to Upgrade from Release 3.1.0 to Release 3.1.1

Perform the following procedure to upgrade your IP camera to Release 3.1.1 only if your IP camera part number is 74-9125-02-02 or 74-9126-02 and the firmware release on the IP camera is 3.1.0. Otherwise, use the procedure in the “[Upgrading to Release 3.2.4](#)” section on page 2.



Note

You can find the IP camera part number listed on the camera user interface Home window, under the General Information area.

Procedure

Step 1 Take these actions to obtain the upgrade hot fix utility:

- a. Go to this URL:
<http://www.cisco.com/cisco/software/release.html?mdfid=282582478&flowid=31387&softwareid=282090156&os=Linux&release=2.4.0&reind=AVAILABLE&rellifecycle=&reltype=latest>
- b. From the navigation pane, choose **All Releases > 3 > 3.1.1**.
- c. Download the upgrade hot fix utility file named **4xxxE-HotFixUtilityInstallerV3.1.1.msi**.
- d. Log in and follow the on-screen prompts to download the upgrade hot fix utility file to your PC.
- e. Close Internet Explorer.

Step 2 Double-click the **4xxxE-HotFixUtilityInstallerV3.1.1.msi** file and follow the on-screen prompts to install the utility on your PC.

During the installation process, the installer adds the Hot Fix Utility icon to your desktop.

Step 3 Double-click the **Hot Fix Utility** icon to open the utility.

Step 4 Take these actions to upgrade a single IP camera:

- a. Click **Single Camera**.
- b. Enter the IP address, admin password, and SSH password for the IP camera to be upgraded.
- c. Click **Upgrade**.

Do not power down the IP camera during the upgrade procedure.

After you upgrade the firmware, the IP camera automatically restarts. It retains all configuration information.

Step 5 Take these actions to upgrade multiple IP cameras:

- a. Using a plain text editor, create and save an input file containing a list of all cameras to be upgraded.

Each line in the input file must contain the IP address, password, and SSH password (separated by space characters) for an IP camera to be upgraded. The following example shows entries for five IP cameras as they should appear in an input file:

```
192.168.1.101 password1 SSHpass1
192.168.1.102 password2 SSHpass2
192.168.1.103 password3 SSHpass3
192.168.1.104 password4 SSHpass4
192.168.1.105 password5 SSHpass5
```

- b. Click **Multiple Cameras**.
- c. Click **Input File**, choose the input file saved in Step 6a, and click **Open**.
- d. Click **Upgrade**.

Do not power down any of the IP cameras during the upgrade procedure.

After you upgrade the firmware, the IP cameras automatically restart. They retain all configuration information.

Step 6 Go to the [“Upgrading to Release 3.2.4” section on page 2](#) to upgrade your IP camera to Release 3.2.4.

Limitations and Restrictions

The following limitations and restrictions apply to firmware release 3.2.4 on 4300E and 4500E high definition IP cameras:

- The browser logs out of the Analytics web UI after prolonged inactivity.

Caveats

Table 1 describes the caveats that are resolved in this release.

Table 1 *Caveats Resolved in this Release*

Identifier	Description
CSCtt42352	Simplified log collection from 4xxxE camera interface
CSCue21713	Analytics alert HTTP POST Request-line has undue trailing space
CSCuf90739	Support of camera GUI using IE 9/10 32-bit clients in Windows 7
CSCuh52835	CVIS-IPC-4500 stops streaming and responding to network requests
CSCui01228	Analytics parameters are not getting updated after calibration
CSCuj70419	Hard-coded Credentials for Analytics page
CSCuo37283	Video Surveillance 4300E/4500E HD IP Cameras vulnerable to CVE-2014-0160

Table 2 describes the caveats that are open in this release.

Table 2 *Caveats Open in this Release*

Identifier	Description
CSCtf87756	Users sometime logged out after resetting the camera when using static IP addresses
CSCtg22847	Camera UI hotspot Pan/Tilt command does not work correctly in certain resolutions
CSCtg73910	PEAP authentication fails when using Validate Server Certificate option
CSCtg76338	When using e-mail notification for motion events, if the e-mail server is unreachable, video stops streaming
CSCtg93230	Change in video resolution changes motion detection area
CSCtj68155	In Edit mode, existing rules may not display in Analytics web UI
CSCtk75349	Missing duplex and power parameters in CDP
CSCto34506	DirectShow setup may sometimes fail
CSCto40637	Video distortion may occur when viewing multiple cameras on the same PC
CSCtn22813	H.264 video may stutter in Web UI if AAC audio codec is enabled

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.



Note

Bug Search Tool is the successor to the Bug Toolkit.

To access the Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

Procedure

- Step 1** To access the Bug Search Tool, go to <https://tools.cisco.com/bugsearch/>
- Step 2** Log in with your Cisco.com user ID and password.
- Step 3** To look for information about a specific problem, enter the bug ID number in the **Search For** field, then press **Enter**.
- Step 4** To look for information if you do not know the bug ID number, enter keywords which search for text matches in the following sections of a bug:
- headline/title
 - release note text
 - product
 - known affected releases/ known fixed releases:
-

For more information about the Bug Search Tool, click **Help** on the main Bug Search Tool page:

<https://tools.cisco.com/bugsearch/>

Related Documentation

For additional information about the Cisco Video Surveillance IP camera, see the *Installation Guide* and *Configuration Guide* for your IP camera. The documentation is available at this URL:

www.cisco.com/go/ipcamera

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.