Cisco IOS Release 15.9(3)M6b - Release Notes for Cisco IR8x9 Industrial Integrated Services Routers

First Published: 2022-12-06

Last Modified: 2022-12-20

Introduction

The following release notes support the Cisco IOS 15.9(3)M6b release. These release notes are updated to describe new features, limitations, troubleshooting, recommended configurations, caveats, and provide information on how to obtain support and documentation.

PSIRT ADVISORY

IMPORTANT INFORMATION - PLEASE READ!

FPGA and BIOS have been signed and updated to new versions.

For the 15.9 Release Train, this image (15.9-3.M) is considered as the baseline. Downgrade is **STRICTLY UNSUPPORTED** and bundle install to previous releases (158-3.M2a/157-3.M4b/156-3.M6b) will cause an error and fail if attempted. Any manual downgrade [non bundle operations] will impair router functionality thereafter.

Note After upgrading to this release, make sure to delete any old image files that may still be in the flash: filesystem. This will prevent an unintended IOS downgrade.

For additional information on the PSIRT see the following:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot

Image Information and Supported Platforms

Note You must have a Cisco.com account to download the software.

Cisco IOS Release 15.9(3)M6b includes the following Cisco IOS images:

IR8x9

System Bundled Image: ir800-universalk9-bundle.SPA.159-3.M6b

This bundle contains the following components:

- IOS: ir800-universalk9-mz.SPA.159-3.M6b
- Guest Operating System: ir800-ref-gos.img.1.15.0.8.gz
- Hypervisor: ir800-hv.srp.SPA.3.1.33
- FPGA: 2.B.0
- BIOS: 28
- MCU Application: 53

Software Downloads

This section contains the following:

IR800 Series

The latest image files for the IR800 product family can be found here:

https://software.cisco.com/download/navigator.html?mdfid=286287045&flowid=75322

Click on the 809 or 829 link to take you to the specific software you are looking for.

Important MANUAL [non-bundle] DOWNGRADE IS STRICTLY PROHIBITED. For newer releases with the PSIRT fix - while bundle downgrade to 158-3.M2a/157-3.M4b/156-3.M6b is supported, manual downgrade is unsupported.

Note On the IR8x9 devices, the IR800 bundle image can be copied via Trivial File Transfer Protocol (TFTP) or SCP to the IR800, and then installed using the bundle install flash:<*image name*> command. The IR800 <image>.bin file can NOT be directly booted using the boot system flash:/image_name. Detailed instructions are found in the Cisco IR800 Integrated Services Router Software Configuration Guide .

Note On the IR8x9 devices, the cipher **dhe-aes-256-cbc-sha** (which is used with the commands **ip http client secure-ciphersuite** and **ip http secure-ciphersuite**) is no longer available in IOS 15.6(3)M and later as part of the weak cipher removal process. This cipher was flagged as a security vulnerability.

IR809

The IR809 link shows the following entries:

- IOS Software

- ir800-universalk9-bundle.<version> .bin
- ir800-universalk9_npe-bundle.<version> .bin

- IOx Cartridges
  - Yocto 1.7.2 Base Rootfs (ir800_yocto-1.7.2.tar)
  - Python 2.7.3 Language Runtime (ir800_yocto-1.7.2_python-2.7.3.tar)
  - Azul Java 1.7 EJRE (ir800_yocto-1.7.2_zre1.7.0_65.7.6.0.7.tar)
  - Azul Java 1.8 Compact Profile 3 (ir800_yocto-1.7.2_zre1.8.0_65.8.10.0.1.tar)

IR829

The IR829 link shows the following entries:

Software on Chassis

- IOS Software
  - ir800-universalk9-bundle.<version> .bin
  - ir800-universalk9_npe-bundle.<version> .bin

- IOx Cartridges
  - Yocto 1.7.2 Base Rootfs (ir800_yocto-1.7.2.tar)
  - Python 2.7.3 Language Runtime (ir800_yocto-1.7.2_python-2.7.3.tar)
  - Azul Java 1.7 EJRE (ir800_yocto-1.7.2_zre1.7.0_65.7.6.0.7.tar)
  - Azul Java 1.8 Compact Profile 3 (ir800_yocto-1.7.2_zre1.8.0_65.8.10.0.1.tar)

AP803 Access Point Module

- Autonomous AP IOS Software
  - WIRELESS LAN (ap1g3-k9w7-tar.153-3.JH1.tar)

- Lightweight AP IOS Software
  - WIRELESS LAN (ap1g3-k9w8-tar.153-3.JH1.tar)
  - WIRELESS LAN LWAPP RECOVERY (ap1g3-rcvk9w8-tar.153-3.JH1.tar)

Warning about Installing the Image

Note The bundle can be copied via Trivial File Transfer Protocol (TFTP), or Secure Copy Protocol (SCP) to the device, and then installed using the bundle install flash:<*image name*> command. The bin file can NOT be directly booted using the boot system flash:/image_name.

Caution MANUAL [non-bundle] DOWNGRADE IS STRICTLY PROHIBITED.

Known Limitations

This release has the following limitations or deviations from expected behavior:

Space Limitation

The device requires a minimum 30MB additional space in the flash: file system before attempting an upgrade, or a downgrade between releases. Otherwise, the FPGA/BIOS will not have enough space to store files and perform the upgrade. In these current releases, the bundle installation will not display a warning, but future releases from September 2019 going forward will have a warning.

CSCvq88011 - IR809, IR829

Bundle install should internally handle “firmware downgrade enable” check

Symptoms: If you manually downgrade hypervisor and IOS only from releases (159-3.M+, 158-3.M3+, 156-3.M7+, 157-3.M5+) to the releases (158-3.M2a, 157-3.M4b, 156-3.M6b), the router will be stuck in a boot loop.

Workaround: If you use the recommended 'bundle install' to downgrade, the process will run correctly.

Major Enhancements

This section provides details on new features and functionality available in this release. Each new feature is proceeded by the platform which it applies to.

Image Recovery from Backup Partition

This feature is available for recovering the router in the absence of an IOS image in flash or possible flash corruption. This feature fixes the CSCwd30188 caveat. During bundle image install, the IOS image is backed up in a hidden partition. On boot up, the router checks for the presence of the IOS image in flash. If the IOS image is present in flash, the normal boot up process will proceed. If the IOS image is absent in flash, the IOS image which is backed up will be copied to flash, and continues to boot up. This prevents the router failing to boot and falling into boot prompt.

The ignition graceful shutdown time has also been increased to 120 seconds.

Note An additional reload is required after the router is upgraded from FND for the image backup.

Related Documentation

The following documentation is available:

- Cisco IOS 15.9M cross-platform release notes

- All of the Cisco IR800 Industrial Integrated Services Router documentation
- All of the Cisco CGR 1000 Series Connected Grid Routers documentation
- IoT Field Network Director
- Cisco IOx Documentation
- Cisco IOx Developer information

Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account .

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ .

Open Caveats

The following table lists open caveats for Cisco IOS Release 15.9(3)M6b:

Item	Platform	Description
CSCwc00866	IR829	Modem 4G reset when receiving CTRL-C from an application. **Symptoms**: 4G Modem is reset when receiving in the break sequence Ctrl + C in the NMEA interface from an IOx app. **Workaround**: Use another break sequence (CTRL-^ then type x then disconnect) to properly disconnect from an existing session.

Resolved Caveats

Cisco IOS Release 15.9(3)M6b has no resolved caveats.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.