Cisco IOS Release 15.8(3)M2 - Release Notes for Cisco IR800 Industrial Integrated Services Routers and Cisco CGR1000 Series Connected Grid Routers

The following release notes support the Cisco IOS 15.8(3)M2 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.

Last Updated: August 2, 2021

First Published: March 30, 2019

Contents

This publication consists of the following sections:

Image Information and Supported Platforms

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

Cisco IOS Release 15.8(3)M2 includes the following Cisco IOS images:

IR8x9

- System Bundled Image: ir800-universalk9-bundle.SPA.158-3.M2

  This bundle contains the following components:

  - IOS: ir800-universalk9-mz.SPA.158-3.M2
  - Guest Operating System: ir800-ref-gos.img.1.8.4.1.gz
  - Hypervisor: ir800-hv.srp.SPA.3.0.77
  - FPGA: 2.7.0

  - BIOS: 23
  - MCU Application: 33

IR807

- IOS Image: ir800l-universalk9-mz.SPA.158-3.M2

CGR1K

- System Bundled image: cgr1000-universalk9-bundle.SPA.158-3.M2
  - IOS Version: cgr1000-universalk9-mz.SPA.158-3.M2
  - Guest Operating System: cgr1000-ref-gos.img.1.8.2.1.gz
  - Hypervisor: cgr1000-hv.srp.SPA.3.0.37
  - FPGA: 2.9.0
  - BIOS: 15

Software Downloads

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 807, 809 or 829 link to take you to the specific software you are looking for.

IR807

The IR807 link shows the following entries:

- ir800l-universalk9-mz.SPA.*<version>*.bin
- ir800l-universalk9_npe-mz.SPA.*<version>*.bin

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)

Note: On the IR8x9 devices, the ir800-universalk9-bundle.SPA.158-3.M bundle 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-universalk9-bundle.SPA.158-3.M.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.

CGR1K Series

The latest image file for the CGR 1000 Series Cisco IOS image is:

https://software.cisco.com/download/navigator.html?mdfid=284165761&flowid=75122

For details on the CGR1000 installation, please see:

http://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/ios/release/notes/OL-31148-05.html#pgfId-9

Warning about Installing the Image

Note: The bundle can be copied via Trivial File Transfer Protocol (TFTP) or 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`.

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.

IR809 and IR829: MIB support for Gyroscope and Accelerometer

A new MIB/OID is available to support the following SNMP operations:

- SNMPwalk: snmpwalk is used to fetch all values of a sub tree under the MIB table or value of particular OID.
- SNMPget: snmpget is used to fetch the value of a particular OID.

The entity OID value is iso.3.6.1.4.1.9.12.3.1.8.230.

The **show platform gyroscope** command gives information about this MIB.

IR829M: MIB support for mSATA Wear Ratio and Usage

mSATA functionality was added to the IR829 product line to add extra storage in the15.8.3M release. The PID IR829M has mSATA support available in the device inventory detail. The following table shows the IR829M SKU with the OID:

Table 1 mSATA OIDs

SKU	OID
IR829M-2LTE-EA-BK9	1.3.6.1.4.1.9.1.2610
IR829M-2LTE-EA-AK9	1.3.6.1.4.1.9.1.2610
IR829M-2LTE-EA-EK9	1.3.6.1.4.1.9.1.2610
IR829M-LTE-EA-AK9	1.3.6.1.4.1.9.1.2673
IR829M-LTE-EA-BK9	1.3.6.1.4.1.9.1.2673
IR829M-LTE-EA-EK9	1.3.6.1.4.1.9.1.2673
IR829M-LTE-LA-ZK9	1.3.6.1.4.1.9.1.2609

As part of this enhancement, SNMP support has been added for the following mSATA parameters on the IR829M:

- lifetime remaining (wear leveling)
- memory usage for the mSATA SSD

As part of this enhancement, further SNMP support has been added. There is a new OID name cevMsataWIIR829 in the existing MIB CISCO-ENTITY-VENDORTYPE-OID-MIB.my under the cevModuleCommonCards functional group.

For example:

cevMsataWIIR829 OBJECT IDENTIFIER ::= { cevModuleCommonCards 689 } -- mSATA wear ratio and usage for IR829.

The entity OID value is iso.3.6.1.4.1.9.12.3.1.9.2.689

The **show platform msata** command gives information about this MIB.

Example: Actual OID and output of SNMP get/walk on OID

<OID> = STRING: " Lifetime Remaining: 99%, Usage: 30%"

Feature Details

The following conditions must be met before performing SNMP requests on the IR829M:

- An active mSATA module must be in the IR829M router.
- Verify this using the **show platform msata** CLI.

Feature Assumptions

- This feature is supported on the IR829M only.
- After a router reload it will take approximately 5 minutes before mSATA data will be populated again. Only SNMP get is allowed on OID cevMsataWIIR829 and is marked as read-only. Setting its value will not be allowed.
- Configurations to enable SNMP on IR800 are necessary for fetching MIB value.

IR809 and IR829: PNP Image Upgrade from FND

When a Cisco IR8x9 is powered on for the first time, the PnP agent process running on the IOS wakes up in the absence of the startup config and attempts to discover the address of the PnP server. The PnP agent uses methods like DHCP and DNS to acquire the desired IP address of the PnP server. Upon successfully acquiring the IP address, the PnP agent initiates a long lived, bidirectional layer 3 connection with the server, and waits for a message from the server. The PnP server application sends messages to the agent requesting for information and services to be performed on the device. The PnP server application sends the required configurations and optionally IOS image to the device.

The Cisco Plug and Play Connect cloud service works with your Smart Account and the Cisco Network Plug and Play solution to provide automatic plug and play server discovery when other methods such as DHCP or DNS are not available.

For more information go to the Plug and Play Connect webpage.

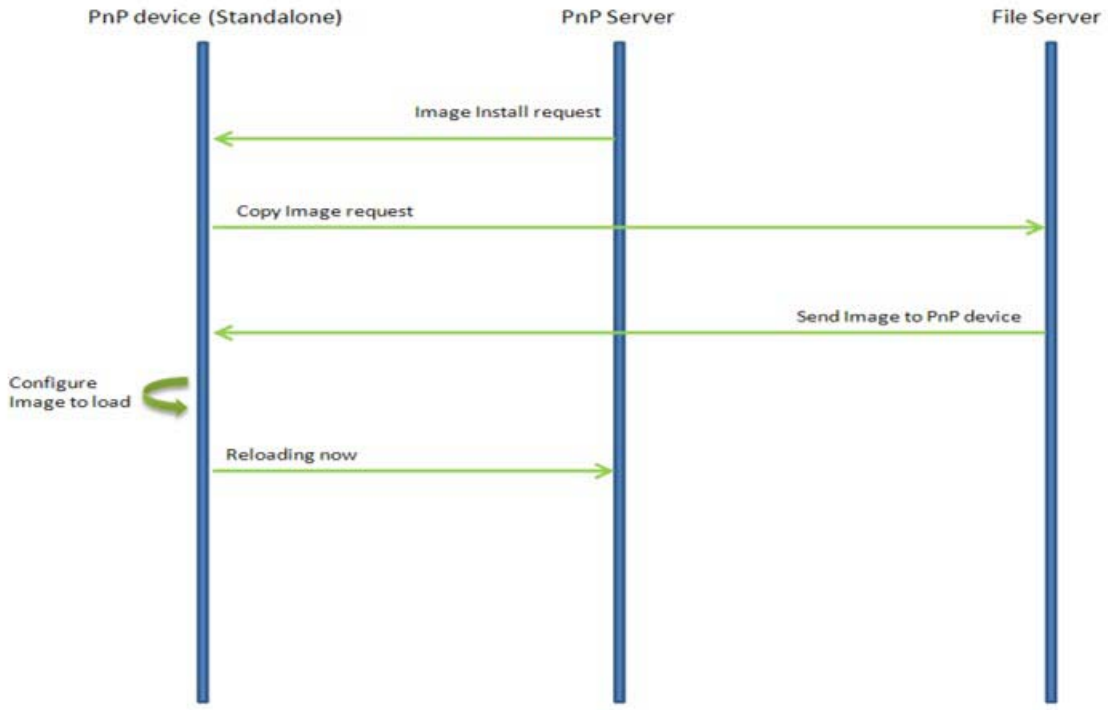
Image Installation

Image Installation service enables a PnP-enabled device to perform an image upgrade upon receiving a request from the PnP Server. The following operations are performed in sequence to successfully load the device with the new image:

1. PnP Server (FND) initiates the upgrade.
2. PnP Device will check the version of the image to be upgraded, and determine if it is a later version than the one the device is booted up with.
3. PnP Device will make a request for copying the image.
4. PnP Device will get the image and its details from PNP agent.
5. Configure the device to load the new image on next reload.
6. Reload the device.

Figure 1illustrates the message flow for a standalone device

Figure 1 PnP Message Flow



The PnP Agent on the device receives a request from the PnP Server, parses the XML payload, and identifies the request as an Image Upgrade request. It then creates an Image Install process, which identifies the request as a Standalone Image Install request.

Based on the fields populated, PnP Image Install will perform the following operations:

- Copy the image from the file server to a local disk. All the information about the file server, Image location, and destination is populated.
- Once the Image is copied, it needs to be configured to load next time the device reloads. For this operation, the 'boot system' CLI is configured in the startup-config.
- The device now sends a message to the PnP Server that it is undergoing a reload.

Feature Assumptions

- This feature is support on the IR809 and IR829 starting from Field Network Director version 4.2.
- Updated PID exists in the PnP Server for new platforms. For end-to-end PnP solution to work, the PnP-server needs to be updated for the specific PID of each new platform.
- The feature supports image upgrade for only bundle image on the IR8x9 platform.
- Upgrade starts upon a request from PnP Server Application.
- No new PnP CLIs will be added as part of this enhancement.

Related Documentation

The following documentation is available:

- Cisco IOS 15.8M cross-platform release notes:

  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/15-8m/release/notes/15-8-3-m-rel-notes.html

- All of the Cisco IR800 Industrial Integrated Services Router documentation can be found here:

  http://www.cisco.com/c/en/us/support/routers/800-series-industrial-routers/tsd-products-support-series-home.html

- All of the Cisco CGR 1000 Series Connected Grid Routers documentation can be found here:

  http://www.cisco.com/c/en/us/support/routers/1000-series-connected-grid-routers/tsd-products-support-series-home.html

- IoT Field Network Director

  https://www.cisco.com/c/en/us/support/cloud-systems-management/iot-field-network-director/products-installation-and-configuration-guides-list.html

- Cisco IOx Documentation is found here:

  https://www.cisco.com/c/en/us/support/cloud-systems-management/iox/tsd-products-support-series-home.html

- Cisco IOx Developer information is found here:

  https://developer.cisco.com/docs/iox/

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.

Cisco IOS Release 15.8(3)M2

The following sections list caveats for Cisco IOS Release 15.8(3)M2:

Open Caveats

- **CSCvp74268 - IR809 and 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 aboot loop.

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

Note: Future releases 159-3.M+, 158-3.M3+, 156-3.M7+, 157-3.M5+ have this issue resolved. Manual and bundle install work, although bundle install continues to be the recommended option for full functionality.

- **CSCvo17731 - IR829 Platform**

  PnP: failed to upgrade image for IR829M router during onboarding on DNAC.

  Symptoms: For an IoT device IR829 with Plug and Play on DNAC, if you upgrade the image during the Plug and Play process, the image upgrade fails.

  Conditions: This problem occurs when creating a Plug and Play project with SWIM (image upgrade).

  Workaround: Do not upgrade the image during the Plug and Play on DNAC. After the device is onboarded, use SWIM to perform an image upgrade.

- **CSCvn36295**

  The command show cel 0 firmware does not show the correct output

  Symptoms:

```
Router#show cel 0 firmware
Idx Carrier      FwVersion    PriVersion   Status
1   ATT          02.32.07.00  002.066_000  Active
2   GENERIC      02.24.05.06  002.026_000  Inactive
3   ROGERS       02.20.03.00  000.011_000  Inactive
4   SPRINT       02.20.03.00  002.017_000  Inactive
5   VERIZON      02.30.01.01  002.052_000  Inactive

Firmware Activation mode : AUTO

IR829#show version
Cisco IOS Software, ir800 Software (ir800-UNIVERSALK9-M), Version 15.8(3.0q)M1,ENGINEERING WEEKLY
BUILD, synced to V155_3_M1

exit
```

  Workaround: The show cell 0 hardware command displays the correct output.

- **CSCvo60928**

  Remove SD-card password from CMOS Register

  Symptoms:

  If SD-card password protection is enabled and the CMOS battery dies it will end up on loader mode.

  To confirm this is the issue:

  Boot with tftp or another SD-card and check the clock.

  Anticipated fix in 158-3.M3 [August 2019]

  Workaround:

  1. Take another SD-card with similar CGOS/IOS boot up the system.
  2. Set the SD-card password with the one it had before reload the box.
  3. Confirm the SD-card password if enables.
  4. Insert the old SD-card and reboot the system.
  5. Once it boots up unset the SD-card password.

Resolved Caveats

The following caveats are fixed with this release:

- **CSCvn17649**

  Disable ssh to local guest-os

  Symptom: From Release 15.8(3)M2 onwards, SSH to the Guest-OS (IOx) shell is disabled by default. SSH to the user application will continue to be accessible.

  Conditions: Disabled SSH access to IOx for all privilege users. Only privilege 15 user will be able to do reverse telnet to IOx.

  Workarounds:

  The ssh access can be enabled using a hidden script for PRIV15 users by following command:

  ```
  Router#iox host exec enablesshaccess IR800-GOS-1
  ```

  To again disable ssh access to highest privilege user again, run following command:

  ```
  Router#iox host exec disablesshaccess IR800-GOS-1
  ```

- **CSCvm46645 - IR8x9 Platform**

  [IOX-SS] Change monitrc to allow for infinite tries to restart secure storage

  Symptoms: IOx came up in recovery mode because secure storage service didn't come up.

  Secure storage service log shows it failed to come up due to network connectivity to IOS. However, ping command went through fine when entered manually from Guest OS console.

  Conditions: This is timing related, triggered by the missing IOS configurations needed for Guest OS networking connectivity at device power up. Secure storage service tried to connect to the server on IOS side and gave up after 5 retries.

  Workaround: Restart guest OS VM after the IOS configuration change by " guest-os 1 restart" . Or, save the configuration, and reload the router.

- **CSCvg41652 - IR829 Platform**

  show cellular x/y drop-stats added.

  Note: From Release 15.8(3)M2 onwards, based on request, show cellular drop-stats cli has been added.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.