Cisco IOS Release 15.9(3)M - Release Notes for Cisco IR800 Industrial Integrated Services Routers and Cisco CGR1000 Series Connected Grid Routers

The following release notes support the Cisco IOS 15.9(3)M 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.

Revised: July 30, 2021

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 15.9(3)M includes the following Cisco IOS images:

IR8x9

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

  This bundle contains the following components:

  - IOS: ir800-universalk9-mz.SPA.159-3.M
  - Guest Operating System: ir800-ref-gos.img.1.9.0.5.gz
  - Hypervisor: ir800-hv.srp.SPA.3.0.83

  - FPGA: 2.A.0
  - BIOS: 25
  - MCU Application: 34

IR807

- IOS Image: ir800l-universalk9-mz.SPA.159-3-M

CGR1K

- System Bundled image: cgr1000-universalk9-bundle.SPA.159-3-M
  - IOS Version: cgr1000-universalk9-mz.SPA.159-3-M
  - Guest Operating System: cgr1000-ref-gos.img.1.9.0.3.gz
  - Hypervisor: cgr1000-hv.srp.SPA.3.0.42
  - FPGA: 2.D.0
  - BIOS: 17

Caution: DOWNGRADE TO ANY RELEASE PRIOR TO THIS RELEASE DATE OF 159-3.M [August 2019] IS STRICTLY UNSUPPORTED. MANUAL [non-bundle] DOWNGRADE IS STRICTLY PROHIBITED.

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.`

PSIRT ADVISORY - Secure Boot for CGR1000

IMPORTANT INFORMATION - PLEASE READ!

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

Going forward, for the 15.9 Release Train, this image (15.9-3.M) is considered as the baseline. Downgrade is unsupported. Downgrade is **STRICTLY UNSUPPORTED** and bundle install to previous releases will cause an error and fail if attempted. Any manual downgrade [non bundle operations] will impair router functionality thereafter.

For additional information on the PSIRT see the following:

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

SD Card Warning on the CGR1000

The SD Card password location has been changed, which results in an updated FPGA upgrade. As a result, the user is requested to DISABLE the SD Card password protection just prior to the upgrade process. Once upgraded, the user is requested to re-enable the same. This is **MANDATORY**.

PSIRT ADVISORY - Disable Reverse Telnet on Embedded AP for IR829

With this PSIRT fix, for access point login via wlap-ap0, use static ip addressing only. IP Unnumbered to gigabit ethernet interfaces will not work.

Known Limitations

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

- **For IOx, please do not use the image installed with the bundle!** With this image, the local manager will not work. This has been fixed in the following IOx image download site for IR809 and IR829.

  To download image standalone, please execute the following in exec mode:

  ```
  guest-os 1 image install flash:ir800-ioxvm.img.1.9.0.7.gz
  wr mem
  reload
  ```

- Please ensure there is a minimum 30MB additional space in the flash: file system before attempting an upgrade or 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.

- SSH access to GuestOS:

  SSH to the Guest-OS (IOx) shell is disabled by default.

  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
```

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.

IR829 - MIB Support for Ignition Power Management

MIB (Management Information Base) is a collection of objects in a virtual database that allows Network Managers using Cisco IOS Software to routers and switches in a network. It is a database used for managing the entities in a communication network. The format of the MIB is defined as part of the SNMP. MIB support is already added for various features in IR800 platform for allowing us to fetch configuration detail outside the router.

The SNMP model defines two entities, which works in a client-server mode. The SNMP server is called a SNMP agent. In our case, SNMP server is located on the IR829 router. The client part is the SNMP manager which can be any locally connected machine. The SNMP agent listens to requests coming from the SNMP manager and accordingly gives response. The SNMP manager collects data and display it.

Adding new MIB/OID will requires a unique OID to perform SNMP operations.

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

Ignition Power Management prevents the router from draining the charge of the battery on automotive applications, and keeps the router up and running when the engine is turned off for a predetermined amount of time. This time period is programmable between 60 to 32400 seconds (9 Hours) using the IOS **ignition off-timer** command. The addition of SNMP support for Ignition Power Management includes a new MIB file " CISCO-IPM-MIB.my" with an OID of 1.3.6.1.4.1.9.12.3.1.6.684. The following graphic shows the of an SNMP get/walk on the new OID:

```
snmpwalk -v2c -u test_user 172.27.127.110 iso.3.6.1.4.1.9.12.3.1.6.684 -c test
iso.3.6.1.4.1.9.12.3.1.6.684.1.0.1.0 = STRING: "Status:
Ignition management: Enabled
Input voltage: 12.2 V
Ignition status: Timing ignition off shut down
Shutdown timer: 6215.0 s to off [will begin power down at ~100 sec]

Thresholds:
Undervoltage: 10.5 V
Overvoltage: 32.0 V
Undervoltage timer: 120.0 s
Overvoltage timer: 1.0 s
Ignition-Off timer: 7200.0 s"

snmpget -v2c -u test_user 172.27.127.110 iso.3.6.1.4.1.9.12.3.1.6.684.1.0.1.0 -c test
iso.3.6.1.4.1.9.12.3.1.6.684.1.0.1.0 = STRING: "Status:
Ignition management: Enabled
Input voltage: 12.2 V
Ignition status: Timing ignition off shut down
Shutdown timer: 6215.0 s to off [will begin power down at ~100 sec]

Thresholds:
Undervoltage: 10.5 V
Overvoltage: 32.0 V
Undervoltage timer: 120.0 s
Overvoltage timer: 1.0 s
```

```
Ignition-Off timer: 7200.0 s"
```

Feature Assumptions

- This feature is supported on the IR829 only with OID 1.3.6.1.4.1.9.12.3.1.6.684.
- The SNMPget operation on OID 1.3.6.1.4.1.9.12.3.1.6.684 will display status of Ignition power.
- Only SNMP get/walk/bulkwalk is allowed on OID 1.3.6.1.4.1.9.12.3.1.6.684 and is marked as read-only. SNMP set is not allowed.
- Configurations to enable SNMP on the IR829 are necessary for fetching MIB value.
- Existing CLI **show snmp mib** can be used for checking newly added MIB.
- No new CLI has been added to IOS parser.

IR829 - Ignition Off Timer Range Limitation

With this release, the IR829 Ignition Off-Timer Upper threshold range changed from 7200 seconds to 32400 seconds. This is the hardware limit of the MCU.

During a timed ignition shutdown, there is an under-voltage trigger, under-voltage [120s time down] will be prioritized. If the undervoltage recovers within the first 20seconds, the router will not shutdown and resume operation, but the ignition off-timer counter will reset back to the original configuration and start the countdown from scratch.

There is no functional impact or change needed to existing users and configurations. As a result, MCU Firmware version updated to #34. CLI and functionality have no impact as a result of this addition.

CLI Example:

```
Device(config)#ignition off-timer ?
<240-32400> Off timer delay value in seconds(device begins shutdown ~100sec
before this value)

Example:
Device#show ignition
Status:
Ignition management: Enabled
Input voltage: 19.0 V
Ignition status: Power on
Shutdown timer: 0.0 s to off [will begin power down at ~100 sec]
Thresholds:
Undervoltage: 11.551 V
Overvoltage: 32.0 V
Undervoltage timer: 120.0 s
Overvoltage timer: 1.0 s
Ignition-Off timer: 32400.0 s
```

IR829 - Ignition Undervoltage Setting

Ignition under-voltage setting has been changed to millivolts in the CLI configuration. However, true accuracy is only in deci-volts. Due to a stated machine limitation, configuration options in millivolts are permitted. The following are CLI examples:

```
Device(config)#ignition undervoltage threshold 24 999
WARNING: This new value is higher than (or very close to) the current input voltage (19.0 V) and
setting it might cause the router to shut down shortly. Proceed with the setting?? [yes/no]: yes
```

```
DNAC30(config)#end

Device#show ignition
Status:
Ignition management: Enabled
Input voltage: 19.0 V
Ignition status: Timing low voltage shut down
Shutdown timer: 118.0 s to off [will begin power down at ~100 sec]
Thresholds:
Undervoltage: 24.999 V
Overvoltage: 32.0 V
Undervoltage timer: 120.0 s
Overvoltage timer: 1.0 s
Ignition-Off timer: 32400.0 s
```

CGR1K - AP trouble shooting with Radio reset codes in dot11 layer

AP (Access Point) Radio reset codes are used to trouble shoot why AP radio resets happen. There can be many reasons for a radio reset, either from Normal/Expected causes or Failures. These reset codes for the dot11 layer is designed in such a way that the Last Radio Reset Code along with the Reset Reason and Cause Type is showed in the show command output. For Radio Resets due to failures, the prefix RADIO_FC should be used. For Radio Resets which are intentional/normal, the prefix RADIO_RC should be used.

The following table lists the Radio Reset Codes that are implemented for dot11 layer.

RC/FC Radio Reset Codes	Reset Reason	Cause Type
RADIO_RC_IDB_ENABLE (26)	IDB Enable	Normal
RADIO_RC_IDB_SHUTDOWN (27)	IDB Shutdown	Normal
RADIO_RC_IDB_RESET (10)	IDB Reset	Normal
RADIO_RC_INIT (43)	Radio Init	Normal
RADIO_RC_CLR_CNT (67)	Clear Count	Normal
RADIO_FC_HB_LOST (46)	Interface down due to Lost Heartbeat Count	Failure
RADIO_FC_RESET (2)	Interface down with driver failure	Failure
RADIO_FC_LOAD_TIMEOUT (18)	Load Timeout	Failure
RADIO_FC_BEACON_STUCK (38)	Beacon Stuck	Failure

Feature Assumptions

- Existing CLI **show controllers dot11radio2/1** can be used to check the last radio reset code along with its reason and cause type.
- No new CLI has been added to IOS parser.

- This feature is supported only for CGR platforms.
- For some resets, triggers cannot be found.

Command Output

The following is an example of the show command output:

```
cgr1k(config-if)#do sh controllers dot11radio2/1
    MAC Address            : 44a7.cfd2.8209
    Driver Version         : 4.219 RC77.9
    Firmware Version       : 4.218.188.0
    Country                : US
    Channel Frequency      : 2417 Channel 2
    Power                  : 10 dBm
    Rate set               : 1.0 2.0 5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
    MCS set                : m0 m1 m2 m3 m4 m5 m6 m7
    SSID                   : cisco
    SSID Suppress          : enabled
    Phy Noise              : -89 dBm
    Last Radio Reset Code  : 27
    Last Reset reason      : IDB Shutdown
    Cause Type             : Normal Cause
```

The following is an example of the debug command output:

```
cgr1k(config-if)#debug dot11 all
*Apr 15 12:12:00 [DOT11 DBG] cgr1000_dot11_radio_reset:
Radio reset reason: IDB Enable, Reset Code: 26,
    Cause Type: 0 - Normal Cause
```

CGR1K - SD Card Serial Number in Show Inventory

Previously there was no method to determine what the serial number of an SD Card was other than removing it and reading the number. This release introduces the ability to read information about the SD card encoded in its internal card registries. The **show inventory** command has been updated to display this information.

The following example shows the output from the **show inventory** command:

```
NAME: "SD Card for CGR", DESCR: "Removable SD Card for Cisco Connected Grid Routers"
PID: SD CARD           , VID:    , SN: 0x39d802a6
```

Related Documentation

The following documentation is available:

- Cisco IOS 15.9M cross-platform release notes:

  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/15-9m/release/notes/15-9-3-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 15.9(3)M

The following sections list caveats for Cisco IOS Release 15.9(3)M:

Open Caveats

- **CSCvq88011 - IR829M**

  Disk Space displayed in Local Manager for IOx for 50GB/100GB mSATA storage reflects more than what should be allocated for applications.

  Symptoms: In the IOx Local Manager, when activating an application, if we select > 80% disk space during app activation on mSATA SSDs [IR829M] app activation may take very long and fail with irregularities. This is since CAF uses same disk space for its activities too so may fail as a result.

  Conditions: IOx App Activation May Fail when using >85% of disk space on mSATA SSD on IR829M.

  Workaround: Deploy <80% for example, [on 50GB mSATA, disk space <40GB].

- **CSCvp22063 - IR829**

  Inserting SIM in Slot 1 disables IP connectivity on a working interface Cell 0/0.

  Symptoms: When a SIM is inserted in Slot 1 (Cell 1/0), the first working modem in Slot 0 (Cell 0/0) looses IP connectivity. The cellular 0/0 (related to Slot 0) modem was working before the SIM in Slot 1 was inserted.

  Workaround: Remove and re-insert the SIM in Slot 0 and possibly power cycle the Cell 0/0.

- **CSCvq48056 - IR829**

  Debug ignition does not work.

Workaround: Use show ignition or show ignition register commands for debugging instead.

- **CSCvq71700 - CGR1000**

  Reload-pending status still shows **yes** even after SD Card password is disabled and reloaded.

  Impact: None, just display of status issue.

  Workaround: None

Resolved Caveats

The following caveats are fixed with this release:

- **CSCvo60928 - CGR1000**

  SD Card password lock

  Symptoms: In some scenarios, CMOS batteries would fail to work under extreme cold conditions and lock up SD Card password. As a solution, SD Card password has been moved to different location.

Workaround: None

- **CSCvm68386 - IR829**

  Ignition undervoltage millivolts is not persistent on reload

  Symptoms: Ignition undervoltage threshold setting in millivolts is not persistent on reload. Volt value is intact, only the decimal value is not persistent.

  Workaround: EEM to reconfigure millivolt threshold on device bootup:

```
#conf t
event manager applet ignition_uv_config
event syslog pattern "Process IR800 Test top-level routine exited"
action 1.0 cli command "conf t"
action 1.1 cli command "ignition undervoltage threshold 11 999"
```

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/en/US/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.

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.