Cisco IOS Release 15.9(3)M1 - 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)M1 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:

PSIRT ADVISORY

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.M1) 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.

Note: After upgrading to this release, make sure to delete any old image files that may still be in flash:. 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)M1 includes the following Cisco IOS images:

IR8x9

- System Bundled Image: ir800-universalk9-bundle.SPA.159-3.M1

  This bundle contains the following components:

  - IOS: ir800-universalk9-mz.SPA.159-3.M1
  - Guest Operating System: ir800-ref-gos.img.1.10.0.14.gz
  - Hypervisor: ir800-hv.srp.SPA.3.0.97
  - FPGA: 2.A.0
  - BIOS: 25
  - MCU Application: 34

IR807

- IOS Image: ir800l-universalk9-mz.SPA.159-3-M1

CGR1K

- System Bundled image: cgr1000-universalk9-bundle.SPA.159-3-M1
  - IOS Version: cgr1000-universalk9-mz.SPA.159-3-M1
  - Guest Operating System: cgr1000-ref-gos.img.1.8.2.6.gz
  - Hypervisor: cgr1000-hv.srp.SPA.3.0.54
  - FPGA: 2.D.0
  - BIOS: 17

Caution: DOWNGRADE TO ANY RELEASE PRIOR TO THIS RELEASE DATE OF 159-3.M1 [January 2020] IS STRICTLY UNSUPPORTED. MANUAL [non-bundle] DOWNGRADE IS STRICTLY PROHIBITED. For newer releases with the PSIRT fix - while bundle downgrade to 158-3.M2/157-3.M4b/156-3.M6b is supported, manual downgrade is unsupported.

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.

Caution: DOWNGRADE TO ANY RELEASE PRIOR TO THIS RELEASE DATE OF 159-3.M1 [January 2020] IS STRICTLY UNSUPPORTED. MANUAL [non-bundle] DOWNGRADE IS STRICTLY PROHIBITED. For newer releases with the PSIRT fix - while bundle downgrade to 158-3.M2/157-3.M4b/156-3.M6b is supported, manual downgrade is unsupported.

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.`

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**.

Known Limitations

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

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.

- **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.

- **SSH access to GuestOS disabled:**

From 15.9(3)M1, access to GuestOS through SSH is completely disabled to address vulnerabilities in IOS - GuestOS communication.

However, to access GuestOS, reverse telnet to the GuestOS shell with this command:

```
router#telnet <GOS interface IP> 2070
```

Note: Only privilege 15 user will be able to do reverse telnet to GuestOS.

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.

CGR1240 - Event Logging of Major Battery Backup (BBU) Events

When the AC power source is turned off, the BBU installed in the CGR1240 takes over and keeps providing power to the device. If the BBU is the only power source available (if AC power has not recovered yet), then the BBU will stand for approximately 4 hours if the BBU was fully charged.

At that time, the next BBU on the stack starts providing power to the device. The BBU that reached 0% SoC will then last for a maximum of 21 days before becoming critically discharged. The BBU enters into lockout mode after that point, and can never discharge. Prior to this 21 day limit, the customer should provide an AC power source so that the BBU gets restored and prevented from entering the lockout mode.

This feature tracks how customers maintain the BBU, and ensures that the guidelines for maintaining the BBU units are followed should a warranty replacement be required.

This feature focuses on the tracking of the major events occurring in the BBU and store it in a event log file which gets located in the non-volatile memory so that we can observe the nature and the frequency of the events occurring in the BBU to ensure the proper usage and maintenance of the BBU units installed in the CGR routers.

Initially, all the BBU event status registers are recorded along with the serial number and the timestamp for each BBU installed in the routers. Then for every 15 minutes, the major BBU event status registers are read and if we detect a change in the value, then record all the BBU status registers with the timestamp for each BBU connected.

```
CGR1240#show platform battery event-log

Message:BBU_inital-Data Time :15:54:40 IST Jan 22 2020

BBU_PRESENCE :PRESENT BBU_READY :READY BBU_RESET :NORMAL BBU_INT_L :NORMAL
AC-Status ------ ENABLE ENABLE ENABLE
12-V AC POWER ----12V-GOOD 12V-GOOD 12V-GOOD
Battery-Status --- Idle Full Idle
Ctrl-Override - 0x0 0x0 0x0
Abs-SOC ------- 89 % 100% 85 %
Rel-SOC ------- 89 % 99 % 85 %
Volt------ (mV) 11706 12058 11614
Curr.----- (mA) 0 0 0
Temp.----- ('C) 31 33 31
Amb.Temp-- ('C) 29 34 29
HeaterTemp ('C) 31 33 31
BootloaderStatus-0xB 0xB 0xB
Heater/StatusControl0x0 0x0 0x0
Serial.Nu

Message:Battery-SOC of unit:1 is reachedhiger threshold of 100 Time :15:55:11 IST Jan 22 2020
SOC: Unit:0 - 89 % Unit:1 - 100% Unit:2 - 85 %
```

```
CGR1240#dir flash:
Directory of flash:/

1 drw- 0 Jan 22 2020 15:41:32 +05:30 managed
11 drw- 0 Jan 22 2020 15:41:34 +05:30 eem
12 -rw- 1274 Jan 23 2020 11:18:02 +05:30 bdl-install.log
13 -rw- 9839 Jan 23 2020 12:53:22 +05:30 bbu_event_01.log
```

IR8x9, CGR1000 - Guest-OS Kernel Migration

In release 15.9(3)M1 and beyond, the Guest-OS will utilize Cisco's IOS-XE kernel. The user can seamlessly upgrade from older releases to new with no impact to Application and data.

Security Enhancement

Access to the Embedded Access Point module on the IR829 has been changed. In previous releases, the AP module can be accessed by doing a reverse telnet on all of the Gigabit Ethernet interface from an adjacent reachable machine. From release 15.9(3)M1 gong forward, the access to the AP module is blocked from all the Gigabit Ethernet interfaces. To access the AP module, you will need to configure an IP address to the “wlan-ap 0” interface and then use the following command to access the AP console:

service-module wlan-ap 0 session

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)M1

The following sections list caveats for Cisco IOS Release 15.9(3)M1:

Open Caveats

- **CSCvs77133 – CGR1120, CGR1240**

  LPMR reason is displayed incorrectly. The correct result should be off if the radio is turned off by the user. Instead it shows Low power

  Symptoms: When User initiates an **lte radio off** command under the controller cellular 3/1, the reason displayed should be OFF when the **sh cellular 3/1 radio** command is executed. It displays as Low Power. No functionality impact. Only a Display issue.

  Workaround: None

- **CSCvs67493 – CGR1000**

  CGR1k WiFi is not functional.

  Symptoms: WiFi interface may come up, but on sending traffic, WiFi will go down.

  Workaround: N/A. Plan for fix in upcoming July 2020 release.

Resolved Caveats

- **CSCvq10301**

  Summary: pnp profile device password command has been deprecated. CLI has no security or functional impact, once configured will be treated as a comment and password hidden.

  Workaround: None

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.