Cisco IOS Release 15.9(3)M3 – 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)M3 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.

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 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)M3 includes the following Cisco IOS images:

IR8x9

- System Bundled Image: ir800-universalk9-bundle.SPA.159-3.M3

  This bundle contains the following components:

  - IOS: ir800-universalk9-mz.SPA.159-3.M3
  - Guest Operating System: ir800-ref-gos.img.1.13.0.4.gz
  - Hypervisor: ir800-hv.srp.SPA.3.1.12
  - FPGA: 2.B.0
  - BIOS: 27
  - MCU Application: 34

IR807

- IOS Image: ir800l-universalk9-mz.SPA.159-3-M3

CGR1K

- System Bundled image: cgr1000-universalk9-bundle.SPA.159-3-M3
  - IOS Version: cgr1000-universalk9-mz.SPA.159-3-M3
  - Guest Operating System: cgr1000-ref-gos.img.1.8.2.12.gz
  - Hypervisor: cgr1000-hv.srp.SPA.3.0.59
  - FPGA: 2.E.0
  - BIOS: 18

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: 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.

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 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.

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`.

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

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.

Kernel Migration – IR8x9 and CGR1k

In release 15.9(3)M3 and beyond, the Guest-OS will utilize the latest Cisco XE-Linux kernel (Linux Kernel v5.4) with updated SDKs. The user can seamlessly upgrade from older releases to new with no impact to Application and data.

DNP3 Enhancement in IR800 & CGR

RTU's which are not DNP3 compliant tend to set DIR bit in data link header. This causes the gateway to drop the DNP3 frame even though the rest of the frame is valid. To allow the gateway to accept frames with DIR=1, new CLI will be added to support the exception.

The following is a command example:

scada-gw protocol ignore direction

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)M3

The following sections list caveats for Cisco IOS Release 15.9(3)M3:

Open Caveats

- **CSCvw39209 - IR807**

  GPS Coordinates not acquired after router reload.

  Symptoms: After a reload of the IR807, the GPS coordinates are not fetched. The GPS Status remains in **"**GPS acquiring". Satellite info are also not seen with **show cellular gps detail** command.

  Workaround: The GPS coordinates are fetched correctly after performing a power cycle/modem reset. Planned fix in 159-3.M4.

- **CSCvw70082 - IR807**

  TCP rawsocket connection teardown is observed when sending serial traffic received on Async interface to client socket with latency.

  Symptoms: With delay and bandwidth limit on egress end of IR807 there is drop of packets for serial traffic with TCP connection tear down for Raw-Socket. Even with 1ms delay and bandwidth limit 300 bit/sec, observed TCP connection tear down.

  Workaround: There is no workaround, planned fix in 159-3.M4.

- **CSCvw84782 - CGR1240**

  TAM/ACT2 Write Object Corruption (WPAN and IOS GTK keys mismatch).

  Symptoms: GTK Keys of CG-Mesh PAN present in IOS not matching with the keys present in WPAN module locally as per the IOS Cli command & show wpan commands. The keys entry is blank (0's) for WPAN command cli output. This issue is rarely observed.

  Workaround: Reload the router, planned fix in 159-3.M4.

- **CSCvw81805 - CGR1240**

  WPAN interface missing after a power outage.

  Symptoms: WPAN interface will not be created and not seen in show running config. This is a random issue and observed very rarely.

  Workaround: Reload the CGR1240 router, planned fix in 159-3.M4.

- **CSCvw64192 - CGR1K**

  IOX web server port inaccessible on CGM-SRV due to TCP concurrent connection storm.

Symptoms: When applying TCP maximum concurrent connection storm on IOx https port 8443, the port becomes inaccessible.

Workaround: Reload the CGM-SRV module, planned fix in 159-3.M4.

Resolved Caveats

- **CSCvw62484**

  The IR829 crashes after sustained TCP storm attack on IOx https port

  Summary: ARP processes consume a lot of memory during the TCP Storm reducing the free memory available in the device gradually causing a device crash. Added support for a new CLI **ip arp entry learn <value>** to limit the entries in the ARP table

- **CSCvu74786**

  Lock the nvram variables to be unconfigurable in rommon mode during **no service password recovery**

  Summary: During no service password recovery configuration, if an IOS image is not present or corrupt in flash or manual boot environmental variable is set in IOS mode, or if IOS bootup was disrupted 20 consecutive times, the router will get into rommon-2. From both rommon-1 and rommon-2, the NVRAM variables are locked in order to prevent the configuration of environmental variables. For recovery in such cases, tftp upgrade from rommon1 is still available to end user.

Communications, Services, and Additional Information

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.

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.