Cisco IOS Release 15.9(3)M4 - 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)M4 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)M4 includes the following Cisco IOS images:

IR8x9

- System Bundled Image: ir800-universalk9-bundle.SPA.159-3.M4

  This bundle contains the following components:

  - IOS: ir800-universalk9-mz.SPA.159-3.M4
  - Guest Operating System: ir800-ref-gos.img.1.14.0.6.gz
  - Hypervisor: ir800-hv.srp.SPA.3.1.21
  - FPGA: 2.B.0
  - BIOS: 27
  - MCU Application: 34

IR807

- IOS Image: ir800l-universalk9-mz.SPA.159-3-M4

CGR1K

- System Bundled image: cgr1000-universalk9-bundle.SPA.159-3-M4
  - IOS Version: cgr1000-universalk9-mz.SPA.159-3-M4
  - Guest Operating System: cgr1000-ref-gos.img.1.8.2.18.gz
  - Hypervisor: cgr1000-hv.srp.SPA.3.0.62
  - 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 disable**

  From release 15.9(3)M1going forward, access to GuestOS through SSH is completely disabled to address vulnerabilities in IOS - GuestOS communication. However, in order to access GuestOS, reverse telnet to the GuestOS shell with the following command:

  ```
  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.

Resiliency Changes in Boot Counter - IR8x9:

Due to multiple power fluctuations/under power scenarios in transportation, there are more chances for the router to drop into rommon because of file and file system corruption. There is an existing implementation in which the boot counter will increment up to 20, to boot the IOS image and land in rommon if any failure is detected in booting the IOS image. A change has been introduced in the existing implementation in which the timer value is set between 1 and 1440 seconds which can introduce a delay between every 4th consecutive attempt to boot IOS image.

The following command configures the feature:

```
rommon bootrec_timer <value in secs>
```

WAN Link Recovery - IR807 & C819:

WANMon monitors WAN links (LTE, Ethernet and IPSec tunnels) for failures and triggers a recovery mechanism. A TCL script file named **tm_wanmon.tcl** for WANMon mechanism has been added to the IOS image. This script can be enabled on IOS side to detect wireless link failures and automate recovery actions, such as module reset followed by router reload (if module reset doesn't help to recover the link).

The following command configures the feature:

```
event manager policy tm_wanmon.tcl authorization bypass
```

Cellular and GPS Serviceability for IR8x9:

This feature is available for troubleshooting Cellular and GPS issues in IR8x9 platforms. This serviceability infrastructure will automatically capture additional debug logs, and execute AT commands on certain failure scenarios, and stores the logs in bootstrap partition.

CLI implementations to turn on/off this feature will be under controller cellular. This feature should be enabled and disabled only by Cisco engineers. It is recommended to turn on this feature only if capturing logs with human intervention is difficult.

To enable the serviceability feature, perform the following:

Step	Command or Action	Description
1	**enable** Example: `IR800> enable`	Enables privileged EXEC mode. Enter your password if prompted.
2	**configure terminal** Example: `IR800# configure terminal`	Enters global configuration mode.
3	**Controller cellular** ***<0/1>*** Example: `IR800(config)#controller cellular 0`	Enters Cellular 3G/4G WWAN Cellular controller. <0-1> Is the Controller unit number.
4	**lte modem serviceability** ***<gps|interface-resets|modem-resets|sim>*** Example: `IR800(config-controller)# lte modem serviceability gps`	Enable the CLI for the respective failure.

5	**end**
	Example:
	`IR800(config-controller)# end`
		Returns to privileged EXEC mode.

6	**write memory** Example: `IR800# write memory`	Save the configuration in NVRAM.

To disable the serviceability feature, perform the following:

Step	Command or Action	Description
1	**no lte modem serviceability** ***<gps|interface-resets|modem-resets|sim>*** Example: `IR800(config-controller)# no lte modem serviceability gps`	Disables the serviceability feature.

Known Limitations

Disable the feature once logs have been collected to avoid CPU overhead and space constraints.

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)M4

The following sections list caveats for Cisco IOS Release 15.9(3)M4:

Open Caveats

- **CSCvx42406 - IR829**

  Accessing webserver results in frozen console.

  Symptoms: IR829 Console freezes while accessing the device IP in a web browser https://*<IP>*.

  Workaround: Hard reboot recovers the router. The console recovers completely after the hard reboot, planned fix in release 15.9(3)M5.

- **CSCvz07596 - IR829**

  Symptoms: During the DoS attack, CAF is restarting and randomly multiple CAF sessions are getting created.

  Workaround: Manually kill the additional CAF processes in GOS, planned fix in 15.9(3)M5.

Resolved Caveats

- **CSCvw39209 - IR807**

  GPS Coordinates not acquired after router reload.

  Summary: After reloading IR807, the GPS coordinates are not fetched and the GPS status remains in "GPS Acquiring".

- **CSCvw70082 - IR807**

  TCP raw socket connection tear-down is observed when sending serial traffic received on Async interface to client socket with latency.

  Summary: 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.

- **CSCvw84782 - CGR1240**

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

  Summary: 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.

- **CSCvw81805 - CGR1240**

  WPAN interface missing after a power outage.

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

- **CSCvw64192 - CGR1000**

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

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

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.