Cisco IOS Release 15.9(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 15.9(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.

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 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)M2 includes the following Cisco IOS images:

IR8x9

- System Bundled Image: ir800-universalk9-bundle.SPA.159-3.M2

  This bundle contains the following components:

  - IOS: ir800-universalk9-mz.SPA.159-3.M2
  - Guest Operating System: ir800-ref-gos.img.1.11.0.5.gz
  - Hypervisor: ir800-hv.srp.SPA.3.1.6
  - FPGA: 2.B.0
  - BIOS: 26
  - MCU Application: 34

IR807

- IOS Image: ir800l-universalk9-mz.SPA.159-3-M2

CGR1K

- System Bundled image: cgr1000-universalk9-bundle.SPA.159-3-M2
  - IOS Version: cgr1000-universalk9-mz.SPA.159-3-M2
  - Guest Operating System: cgr1000-ref-gos.img.1.8.2.7.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.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`.

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.

AT&T FirstNet Support for the IR829

FirstNet is a spectrum set aside by the US government for first responders (fire, police, & ambulance crews).

For the new IR829 PID**,** the user is prompted to configure strong enable secret after factory default boot up, along with the below default security features.

- Telnet and HTTP – Disabled by Default
- SSH and HTTPS – Enabled by Default
  - To configure SSH, refer to the following:

    https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/security/configuration_guide/b_sec_152ex_2960-x_cg/b_sec_152ex_2960-x_cg_chapter_01001.html#d43017e591a1635
  - To configure HTTPS, refer to the following:

    https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/https/configuration/15-mt/https-15-mt-book/nm-https-sc-ssl3.html#GUID-3501A644-E52A-40F4-A5D2-E7D4853B96B7
- Login delay and login block – Enabled by Default. See the following table:

Command	Description
login delay *<seconds>* Example: `login delay 3`	When the user authentication fails in Telnet/SSH/HTTP, the next login prompt will appear to the user after a specified amount of time in seconds. The feature is enabled after factory default boot up. The default value is 3 seconds.
login block-for *<seconds>* attempts *<tries>* within *<seconds>* Example: `login block-for 60 attempts 3 within 30`	When the user authentication fails in Telnet/SSH/HTTPS for a specific number of attempts within a period a time in seconds, then further connection attempts are refused for a particular amount of time. The feature is enabled after factory default boot up. The default behavior is when the user authentication fails in SSH/Telnet/HTTP for 3 attempts within 30 seconds, then the connection request to that service is blocked for 60 seconds.

- When the router boots up in factory default mode, the user is prompted to configure a strong enable secret with the following strength checks:
  - Minimum length of 10 characters
  - Have at least one lower case, one upper case and one numerical digit
  - Should not contain the word cisco

If the user ignores the Initial configuration dialog box by entering NO, or presses CTRL+C at the dialog box to quit, the enable secret configuration is displayed until the user configures the strong enable secret.

Verifying the enable secret Prompt

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [IR800]: IR800

  The enable secret is a password used to protect
  access to privileged EXEC and configuration modes.
  This password, after entered, becomes encrypted in
  the configuration.

  ------------------------------------------------
  secret should be of minimum 10 characters with
  at least 1 upper case, 1 lower case, 1 digit and
  should not contain [cisco]
  ------------------------------------------------
  Enter enable secret: ***********
  Confirm enable secret: ***********

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.

  Enter enable password: <password>


  The virtual terminal password is used to protect
  access to the router over a network interface.

  Enter virtual terminal password: <password>

  The iox hypervisor password is used to protect access to
  the VDS. This password will be ENCRYPTED.
  Enter VDS root password []:

Current interface summary

Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0           unassigned      YES unset  administratively down down
GigabitEthernet1           unassigned      YES unset  down                  down
GigabitEthernet2           unassigned      YES unset  down                  down
GigabitEthernet3           unassigned      YES unset  down                  down
GigabitEthernet4           unassigned      YES unset  down                  down
Wlan-GigabitEthernet0      unassigned      YES unset  up                    up
Async0                     unassigned      YES unset  up                    down
Async1                     unassigned      YES unset  up                    down
GigabitEthernet5           unassigned      YES unset  administratively down down
Cellular0/0                unassigned      YES TFTP   down                  down

[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
```

```
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
```

Verifying the Status of SSH

```
IR800#show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
```

Verifying the Status of HTTP

```
IR800#show ip http server status
HTTP secure server status: Enabled
HTTP secure server port: 443
```

No Service Password Recovery on the IR809 and IR829

The No Service Password-Recovery feature is a security enhancement, that when enabled, prevents anyone with console access from using a break sequence (Control+C) during bootup to enter into rommon.

The following events will cause the router will go into rommon mode as standard behavior:

- There is a corrupt or missing IOS image in the flash
- Manual boot setting was done in IOS mode
- IOS bootup was disrupted 20 consecutive times

In an upcoming release, Cisco will lock the environment variable to prevent file access in rommon mode, to further secure the device.

Enabling no service password-recovery

Prerequisites: Ensure bundle install process is used to upgrade to this image. Same as with all other features.

Refer to the following table for steps to enable the feature:

	Command or Action	Description
1	**enable** Example: `IR800>enable`	Enables privileged EXEC mode. Enter your password if prompted.
2	**show version** Example: `IR800#show version`	Displays information about the system software, including configuration register settings.

	Command or Action	Description
3	**configure terminal** Example: `IR800#configure terminal`	Enters global configuration mode.
4	**config-register *<value>*** Example: `IR800(config)#config-register 0x102`	(Optional) Changes the configuration register setting. If necessary, change the configuration register settings on the router to set to autoboot.
5	**no service password-recovery** Example: `IR800(config)#no service password-recovery`	Disables password-recovery capability at the system console.
6	**exit** Example: `IR800(config)#exit`	Exits global configuration mode and returns to EXEC mode.
7	**write memory** Example: IR800#**write memory**	Save the configuration in NVRAM

Disabling no service password-recovery

Disable the **no service password-recovery** feature by configuring **service password-recovery**

```
IR800(config)#service password-recovery
```

Known Limitations

Always disable the feature (execute **service password-recovery**) before downgrading to an image that does not support this feature.

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)M2

The following sections list caveats for Cisco IOS Release 15.9(3)M2:

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

- **CSCvu74786**

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

  Symptoms: 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. Plan to lock the nvram variables configuration in the rommon prompts. This caveat will be resolved in next release.

  Workaround: Not Applicable

Resolved Caveats

None at this time.

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.