



Cisco IOS Release 15.8(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 15.8(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:

- [Image Information and Supported Platforms, page 1](#)
- [Software Downloads, page 2](#)
- [Known Limitations, page 4](#)
- [Major Enhancements, page 4](#)
- [Related Documentation, page 5](#)
- [Caveats, page 5](#)
- [Obtaining Documentation and Submitting a Service Request, page 5](#)

Image Information and Supported Platforms

Note: You must have a Cisco.com account to download the software.

Cisco IOS Release 15.8(3)M4 includes the following Cisco IOS images:

IR8x9

- System Bundled Image: `ir800-universalk9-bundle.SPA.158-3.M4`

This bundle contains the following components:

- IOS: `ir800-universalk9-mz.SPA.158-3.M4`
- Guest Operating System: `ir800-ref-gos.img.1.8.4.1.gz`
- Hypervisor: `ir800-hv.srp.SPA.3.1.2`

Software Downloads

- FPGA: 2.A.0
- BIOS: 25
- MCU Application: 33

IR807

- IOS Image: ir800l-universalk9-mz.SPA.158-3.M4

CGR1K

- System Bundled image: cgr1000-universalk9-bundle.SPA.158-3.M4
 - IOS Version: cgr1000-universalk9-mz.SPA.158-3.M4
 - Guest Operating System: cgr1000-ref-gos.img.1.8.2.1.gz
 - Hypervisor: cgr1000-hv.srp.SPA.3.0.37
 - FPGA: 2.D.0
 - BIOS: 17

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)

Software Downloads

- 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>

Known Limitations

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`.

Known Limitations

- SSH access to GuestOS:

From 15.8(3)M2, 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 preceded by the platform which it applies to.

None for this release.

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 15.8 Release Train, this image (15.8-3.M) is considered as the baseline. Downgrade is **STRICTLY UNSUPPORTED!** A 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>

PSIRT ADVISORY - Disable Reverse Telnet on Embedded AP for IR829

CSCva28270 - 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.

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**.

Related Documentation

The following documentation is available:

- Cisco IOS 15.8M cross-platform release notes:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/15-8m/release/notes/15-8-3-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 15.8(3)M4

The following sections list caveats for Cisco IOS Release 15.8(3)M4:

Open Caveats

None at this time.

Resolved Caveats

None at this time.

Caveats

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.

© 2020 Cisco Systems, Inc. All rights reserved.