Cisco IOS Release 15.7(3)M - Release Notes for Cisco IR800 Industrial Integrated Services Routers and Cisco 1000 Series Connected Grid Routers

The following release notes support the Cisco IOS 15.7(3)M 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.

Contents

This publication consists of the following sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Image Information and Supported Platforms

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

Cisco IOS Release 15.7(3)M includes the following Cisco IOS images:

- System Bundled Image: ir800-universalk9-bundle.SPA.157-3.M

  This bundle contains the following components:

  - IOS: final version 15.7(3)M
  - Hypervisor: 3.0.11
  - FPGA: 2.7.0
  - BIOS: 13
  - MCU Bootloader: 28 (applies only to the IR829)
  - MCU Application: 31
  - Guest Operating System: Cisco-GOS,version-1.4.2.3
- System Bundled image: cgr1000-universalk9-bundle.SPA.157-3.M
  - IOS Version: 15.7(3)M
  - Hypervisor: 3.0.09
  - FPGA: 2.9.0
  - BIOS: 14
  - Guest Operating System: Cisco-GOS,version-1.2.5.2

The latest downloads for the IR809 and IR829 can be found at:

https://software.cisco.com/download/navigator.html?mdfid=286287045&flowid=75322

Click on the 829 or 809 link to take you to the specific software you are looking for.

Software on the Chassis includes:

- IOS Software
- IOx Cartridges
- IOx Fog Node Software

The IR829 also includes downloads for the AP803 Access Point Module:

- Autonomous AP IOS Software
- Lightweight AP IOS Software

The latest image file for the CGR 1000 Series Cisco IOS image is:

https://software.cisco.com/download/navigator.html?mdfid=284165761&flowid=75122

Note The ir800-universalk9-bundle.SSA.157-2.0v.M0.1 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.156-3.M2.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 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.

Caution A problem exists where the MCU upgrade fails to complete and the IR829 stays in bootloader mode. The router will get stuck in ROMMON mode and must be sent back to Cisco with a RMA. The IR829 should only be upgraded to IOS version 15.6(3)M*x*. For example:
If the IR829 is running 15.5(3)M1, DO NOT upgrade to 15.5(3)M2. Go straight to 15.6(3)M*x*.

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-998856

Note Special note for the CGR 2010:
Customers using a 4G card should not update to this release. The 77XX modem is not supported.
More information is available at:
http://www.cisco.com/c/en/us/products/collateral/routers/2000-series-connected-grid-routers/data_sheet_c78_593509.html

Known Limitations

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

On the IR800 series routers, there exists a condition where Cisco Application-hosting Framework (CAF) may not be able to start, and Local Manager/Fog Director/ioxclient connectivity/management will not work. The problem occurs when you have Linux Containers (LXC) or Docker applications deployed prior to version 1.2.4.4 or later (for example: 1.0.0.4, 1.1.0.4, 1.2.4.2).

In order to correct this condition, you will have to uninstall the Docker or LXC applications prior to installing the new IR800 IOX image 1.2.4.4 or later, or the IR800 bundle image 15.6(3)M2 or later.

Then you will need to re-compile/re-image the Docker or LXC applications with the newer kernel version (for example from 3.19 to 4.1.30). At this point, you will be able to deploy them after the new IOX 1.2.4.4 (or later) installation.

Note: Starting with Cisco IOS release 15.6(3)M2 or later, IR800 IOX (either Ref Image or signed Dev-Net image) will be based on MontaVista CGX 2.0.0 Linux with the kernel 4.1.30-rt34-yocto-standard.

Caveat CSCvf76265 crosses over several different IOS software releases, and is a platform driver code issue. It is included here as a known limitation with the IR800 and CGR Industrial Routers.

On both the CGR1000 and IR800, the core dump fails to write into the local flash. The IOS is running as a virtual machine and then hypervisor is running underneath. The local flash is provided by the hypervisor as a virtual disk. When a crash occurs, this virtual disk is no longer available therefore copying to flash will fail. The workaround is to use an ftp server to copy the core dump to.

Major Enhancements

This release includes the following enhancements:

- IOx Radius authentication, page 4
- IOx IPv6 Networking Option, page 4

IOx Radius authentication

This feature allows for enabling the AAA login to IOx applications. There are different options:

- If your device shows **no aaa new-model** in the configuration, it will use local authentication.
- If your device shows **aaa new-model** in the configuration, there are two different methods of authentication.
  - If your device shows **no iox aaa authentication** in the configuration, it will use the default authentication list, for example: "aaa authentication login default".
  - If your device shows **iox aaa authentication WORD** in the configuration, it will use the newly created list/group you specify.
  - To create a login authentication group/list, use **aaa authentication login WORD.** Then specify the name to use for IOX authentication using **iox aaa authentication WORD** For example:

```
IR800#show run | inc aaa
aaa new-model
aaa authentication login default local
aaa authentication login ioxList group radius local <-- implies 1st preference radius,
2nd preference: local login
aaa session-id common
iox aaa authentication ioxList <--to apply the newly created list above
```

Note TACACS+ is unsupported. Only local login and RADIUS are supported.

IOx IPv6 Networking Option

IOx interfaces on IOS now support IPv6 addressing. See the IOx documentation for further information.

Additional New Functionality

Cellular Backoff

Cellular Backoff is a feature introduced in IOS 15.7 for IoT platforms IR800 and CGR1000. It addresses the concerns about Cisco 3/4G router not performing backoff in error handling. When PDP Context activation is failing, modems may receive from a cellular service provider. As a result, when some specific error codes (for example: 29, 33) are received by the modem from a cellular network, the router's IOS incrementally adds interval in sending PDP Context Activation requests and any IP traffic such as not to load service provider network with requests that are known to IOS as failing. Once PDP Context is established and IP traffic is successful, the Cellular Backoff is removed for normal operation.

This back-off implementation will be a generic design and will NOT be specific to a particular service provider. There will be NO IOS CLI command to disable this new feature either.

Related Documentation

The following documentation is available:

- Cisco IOS 15.7M cross-platform release notes:

  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/15-7m/release/notes/15-7-3-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

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 15.7(3)M

The following sections list caveats for Cisco IOS Release 15.7(3)M:

Open Caveats

- **CSCvf13036**

  On the CGR1K, inconsistent RAT preference displays as WCDMA or GLW when UMTS is configured.

  When RAT technology is selected to be 'auto', it may show up on some modem firmware as 'GWL' (ie, GSM, WCDMA, or LTE) as RAT preference under 'show cellular slot radio'. This is a cosmetic issue, and does not affect functionality.

  Workaround: None
- **CSCvb44930**

  On the CGR1K, firmware upgrade fails with an error code 105. Seen on both the MC7430 and MC7455 modems.

  Workaround: Reload the router.

- **CSCvf12166**

  GOS networking fails to come up

  Symptoms: Even on a router reload, GOS IPv6 addressing never gets assigned. GOS networking is completely down.

  Conditions: When encapsulation dot1q is configured on the GOS sub-interface and BVI attached to it, and then 'shut' the interface and change to another physical interface without dot1q.

  Workaround: Default the interface with dot1q encapsulation, even if it is in 'shut' state.

- **CSCvc99738:**

  IKEv2 tunnel fails to come up between Cisco routers after upgrading one router to 15.5(3)S5, 15.5(3)M5

  Symptoms: IKEv2 tunnel negotiation between two Cisco routers fails in IKE AUTH exchange after upgrading one of the routers to 15.5(3)S5 or 15.5(3)M5.

  Conditions:

  1. KEv2 tunnel configured between 2 Cisco routers (IOS or IOS-XE)
  2. IKEv2 Fragmentation enabled and IKEv2 IETF fragmentation being negotiated between the two peers.
  3. One of the routers is upgraded to15.5(3)S5 or 15.5(3)M5.
  4. IKE AUTH packet size exceeds the IKEv2 Fragmentation MTU and hence is fragmented at IKE layer.

  Workaround: Disable IKEv2 Fragmentation, or, upgrade the peer as well to 15.5(3)S5 or 15.5(3)M5

- **CSCvf91570**

  On the CGR1K, Third-party modules may show power sequence error when powering up.

  Conditions: Starting with Cisco IOS version 15.6(3)M1b, whenever a third-party module is powered up, the following power sequence error log message may be generated.

  ```
  CGR1000_JAF1626BLCM(config)#no hw-module poweroff 5
  CGR1000_JAF1626BLCM(config)#
  Sep 11 11:50:45.317 PDT: %CGR1K_SYS-3-MODULE_POWER_SEQ: Module power sequence error,
  slot 5 error 5 data 1101
  ```

  This is due to an enhancement for power sequence error reporting to ensure that Cisco modules are properly powered up. However, for third-party modules, such power sequence error may be safely ignored as long as the module does not have any temperature sensor.

  Workaround: None

- **CSCvf75957**

  Problem Description:

  Bundle install failure/timeout, IOx failure

  Symptoms:

  1. ping to VDS fails:

     ```
     router#ping 127.1.3.1
     ```

  2. bundle install times out
  3. iox applications are not accessible anymore

Conditions:

Typically, when the router is left idle for many weeks and months, there is a possibility to observe this when upgrading to the next software image.

Root Cause:

Root cause was that dual modem logs in VDS were not rotating and size increased in time. Due to lack of memory, bundle install attempts failed. Reload the router before reattempting bundle install and image upgrade.

Issue is seen in all software images supporting dual modem [15.6(3)M and beyond]

Workaround:

Reload IOS and system will recover.

- **CSCvd41974**

  Problem Description:

  On IR829 and IR809 platform, there is a Wpan2 interface shown by default in 15.6(3)M2 and beyond software images.

  Condition:

  The show run command will by default show an additional interface, regardless of whether LoRa modem is attached or not.

```
router#show run int wpan 2
Building configuration...
Current configuration : 78 bytes
!
interface Wpan2
 no ip address
 ieee154 txpower 25
 no ieee154 fec-off
end
```

  Workaround:

  None

- **CSCvf74520**

  Problem Description:

  The IR829 keeps reloading back to IOS when the ignition management is enabled and the ignition is OFF.

  Condition:

  When the ignition management is enabled and the ignition is OFF, the IR829 does not stay shut down when its ignition off-timer expires. It keeps reloading back to IOS, getting shut down again and the same cycle repeats. The battery will be eventually drained due to this repeated cycle.

  Workaround:

  There is no workaround. Customers are recommended to use 15.6(3)M2 to avoid this problem.

Resolved Caveats

The following caveats are fixed with this release:

- **CSCvd70062**

The running-config always shows the `gyroscope-reading enable` setting even if the feature is disabled. The default setting for the gyroscope-reading feature is disabled, and the setting is supposed to be `no gyroscope-reading enable` in the running-config.

Workaround:

Issue the EXEC command **`show platform gyroscope-data`** to check whether the feature is actually enabled or disabled.

- **CSCvd76690**

  Bundle install redundant lengthy time-out right after reload.

  On the IR800 series, right after router reboot, the IOS-VDS hb failure syslog message comes in quite late. Because of this, if the user erroneously tries a bundle install, the following is observed:

  Expected - Bundle install should immediately timeout/fail stating vds not up

  Observation - Bundle install continues for next 15 minutes and then times out.

  Expected - VDS eventually comes up within a minute or two, and can be reached

  Observation - Even though VDS is now accessible, bundle install continues to timeout. So no value add in letting it run.

  Workaround:

  Ping the IP address 127.1.3.1. Proceed with bundle install only if the ping to VDS succeeds.

- **CSCvd74884**

  On repeated reload, MCU reattempts to upgrade application firmware.

  This problem occurs very rarely on the IR800 series. Observed syslog:

  %NOTICE: The system booted with MCU in bootloader mode, which triggers the MCU upgrade.For MCU upgrade, MCU must be in bootloader mode. MCU is going to bootloader mode This might cause System reload.

  Workaround:

  Device eventually comes back up in a couple of reboots.

- **CSCvc53663**

  On the CGR1K series, SSH enabling/disabling for IOX does not work consistently.

  When SSH server is enabled or disabled in GOS VM using the `iox host exec disablessh/enablessh xxxx command`, the operation may randomly fail or succeed.

  Workaround:

  Repeat the command several times until it succeeds.

- **CSCvc12365**

  On the 800 series routers, configured with Dialer Watch configurations, if the interface cellular is up and device is reloaded, the dial-out does not happen and IP does not appear on cellular interface.

  Workaround:

  Perform a shut then noshut on the cellular interface.

- **CSCvc80191**

  On the CGR1K series, an ungraceful IOX shutdown may cause previously running apps to get stuck in deployed or failed state after booting.

  If an app is deployed and running and the device is power-cycled or the GOS VM is ungracefully restarted, the app may be stuck in deployed or failed state after booting.

Workaround:

Uninstall the app prior to power-cycling the router or ungracefully restart the GOS VM. Re-install the app after booting.

- **CSCvc81796**

  Cgroups error message may occasionally show up during apps operations, such as install/uninstall.

  When an app is installed or uninstalled, this error message may show up in the GOS VM console:

  ```
  /software/apps/work/repo-proc# cgroup: cgcreate (762) created nested cgroup for
  controller "memory"
  ```
  which has incomplete hierarchy support. Nested cgroups may change behavior in the future. cgroup: "memory" requires setting `use_hierarchy` to 1 on the root.

  Workaround:

  None

- **CSCvd74257**

  BVI host list detail only shows IPv6 , not IPv4 address.

  On the IR800 series, IPv4 address does not show up in host list detail. Functionally no impact to Guest-OS, user can ping, ssh IOx v4 interface. It is just TPM issue.

  Workaround:

  Reboot router. No functional impact of defect.

- **CSCvd74252**

  SFP-GE-T in IR829 throws traceback as unrecognized device.

  Workaround:

  ```
  conf t
  service internal
  service unsupported-transceiver
  SFP shows up.
  ```

  Sometimes on system reload it recovers as well.

- **CSCvd47333**

  On the IR800 series, GOS restart times out with multiple applications running.

  With the new graceful shutdown of applications implementation, CAF takes longer to shutdown the apps. GOS restart times out.

  Workaround:

  Wait for 5 minutes. Applications should come up by themselves.