Cisco ATA 190 Release Notes for Firmware Release 1.2(2)SR2

First Published: 2020-09-16

Cisco ATA 190 Release Notes for Firmware Release 1.2(2)SR2

These release notes support the Cisco Analogue Telephone Adapter (ATA) 190 running Firmware Release 1.2(2)SR2.

The following table lists the support and protocol compatibility for the Cisco ATA 190.

Table 1: Cisco ATA 190 Support and Firmware Release Compatibility

Cisco IP Phone	Protocol	Support Requirements
Cisco ATA 190	SIP	Cisco Unified Communications Manager (Unified CM) 10.5(1) and later Cisco Unified Communications Manager DST Olsen version D or later SRST 8.0 (IOS load 15.1(1)T) and above
Cisco ATA 190	SIP	Cisco Unified Communications Manager Express (CME) 10.0 (IOS load 15.3(3)M)

Related Documentation

Use the following sections to obtain related information.

Cisco Unified Communications Manager Documentation

See the *Cisco Unified Communications Manager Documentation Guide* and other publications that are specific to your Cisco Unified Communications Manager release. Navigate from the following documentation URL:

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

Cisco Unified Communications Manager Express Documentation

See the Cisco Unified Communications Manager Express publications that are specific to your Cisco Unified Communications Manager Express release. Navigate from the following documentation URL:

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-express/tsd-products-support-series-home.html

Cisco ATA 190 Series Documentation

Refer to publications that are specific to your language and call control system. Navigate from the following documentation URL:

https://www.cisco.com/c/en/us/products/unified-communications/ata-190-series-analog-telephone-adapters/index.html

Installation

Installation Requirements

Before you install the firmware release, you must ensure that your Cisco Unified Communications Manager (Unified CM) is running the latest device pack. After you install a device pack on the Unified CM servers in the cluster, you need to reboot all the servers.

Note If your Unified CM doesn't have the required device pack to support this firmware release, the firmware may not work correctly.

For information on the Unified CM Device Packs, see https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/matrix/CMDP_BK_CCBDA741_00_cucm-device-package-compatibility-matrix.html.

Install the Firmware Release on Cisco Unified Communications Manager

Before you use the Cisco ATA 190 with Cisco Unified Communications Manager (Unified CM) 10.5, or higher, you must install the latest firmware on all Unified CM servers in the cluster.

Besides Unified CM, the Cisco ATA 190 can also work with Cisco Unified Communications Manager Express and Cisco Unified Survivable Remote Site Telephony (SRST). Refer to the Related Documentation, on page 1 section for more information.

Procedure

Step 1 Go to the following URL:
https://software.cisco.com/download/navigator.html?mdfid=268437683&flowid=77852

Step 2 Choose **ATA 190 Series Analog Telephone Adapters** > **ATA 190 Analog Telephone Adapter**.

Step 3 In the Latest Releases folder, choose **1.2(2)SR2**.

Step 4 Select **cmterm-ata190.1-2-2-003_SR2-1.k3.cop.sgn** firmware, click the Download or Add to cart button, and follow the prompts.

Step 5 Click the + next to the firmware file name in the Download Cart section to access additional information about this file. The hyperlink for the Readme file is in the Additional Information section, which contains installation instructions for the corresponding firmware.

Step 6 Follow the instructions in the Readme file to install the firmware.

Install the Firmware Zip Files

Before you use the Cisco ATA 190 with Cisco Unified Communications Manager (Unified CM) 10.5, or higher, you must install the latest firmware on all Unified CM servers in the cluster.

Besides Unified CM, the Cisco ATA 190 can also work with Cisco Unified Communications Manager Express and Cisco Unified Survivable Remote Site Telephony (SRST). Refer to the Related Documentation, on page 1 section for more information.

Procedure

Step 1 Go to the following URL: https://software.cisco.com/download/navigator.html?mdfid=268437683&flowid=77852

Step 2 Choose **ATA 190 Series Analog Telephone Adapters** > **ATA 190 Analog Telephone Adapter**.

Step 3 In the Latest Releases folder, choose **1.2(2)SR2**.

Step 4 Select **cmterm-ata190.1-2-2-003_SR2-1.zip** firmware, click the Download or Add to cart button, and follow the prompts.

Step 5 Click the + next to the firmware file name in the Download Cart section to access additional information about this file. The hyperlink for the readme file is in the Additional Information section, which contains installation instructions for the corresponding firmware.

Step 6 Follow the instructions in the readme file to install the firmware.

Limitations and Restrictions

Manufacturing Installed Certificate Signature and SHA-256 Support

The manufacturing installed certificate(MIC) signature has been updated from SHA-128 with RSA to SHA-256 with RSA. You must update and install the new SHA-2 certificates on the Cisco Unified Communications Manager for secure mode to function. You can download the new certificate from http://www.cisco.com/security/pki/certs/cmca2.cer.

All applications that authenticate the phone MIC should update the MIC, including the following:

- Cisco Unified Communications Manager
- Cisco Unified Survivable Remote Site Telephony
- Cisco Secure Access Control System
- Cisco Identity Services Engine

For additional information about SHA-2 use and support, see *Security Guide for Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html).

Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone audio and, in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

- Administrative tasks, such as an internal port scan or security scan

- Attacks that occur on your network, such as a Denial of Service attack

Caveats

This section describes the resolved and open caveats, and provides information on accessing the Cisco Software Bug Toolkit.

View Caveats

You can search for caveats using the Cisco Bug Search.

Known caveats (bugs) are graded according to severity level, and can be either open or resolved.

Firmware Release 1.2(2)SR2 for Cisco ATA 190 Series doesn't have any open caveats.

Before you begin

To view caveats, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

Procedure

Step 1 Use this URL for the resolved caveats: https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=284883944&rls=1.2(2)SR2&sb=fr&bt=custV

Step 2 When prompted, log in with your Cisco.com user ID and password.

Step 3 (Optional) Enter the bug ID number in the Search for field, then press **Enter**.

Open Caveats

Firmware Release 1.2(2)SR2 for Cisco ATA 190 doesn't have any open caveats.

Resolved Caveats

The following list shows the severity 1, 2, and 3 defects that are resolved for the Cisco ATA 190 Analog Telephone Adapter Release Firmware Release 12.1(2)SR2.

For more information about an individual defect, access the Bug Search toolkit and search for the defect using the Identifier. You must be a registered Cisco.com user to access this online information.

Because defect status continually changes, the table reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit as described in View Caveats, on page 4.

- CSCvp09761 ATA 190 over WAN crashes and unregisters due to illegal memory access in DSP
- CSCvu55523 CVE-2018-0734 CVE-2018-0732 CVE-2018-5407 CVE-2018-0737 Multiple Vulnerabilities in openssl

- CSCvu55519 Linux Kernel get_rock_ridge_filename Function Information Disclosure CVE-2016-4913
- CSCuz33129 ATA190: Need remote restart capability in Web GUI
- CSCvs28822 ATA190 CVE-2019-15666 in linux_kernel
- CSCvs28818 ATA190 CIAM alerts for Linux - CVE-2019-15214
- CSCvs28793 ATA190 CVE-2019-5482 cURL and libcurl tftp_receive_packet() Function Heap Buffer Overflow
- CSCvs28783 ATA190 CVE-2019-3896 Linux Kernel dr_remove_all() Function Double-Free Vulnerability
- CSCvr49341 ATA190 Analog Telephone Adapter Web Access Management Vulnerabilities
- CSCvq19682 Evaluation of ata190 for TCP_SACK

Cisco IP Phone Firmware Support Policy

For information on the support policy for phones, see https://cisco.com/go/phonefirmwaresupport.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)