Release Notes for Cisco Small Business SPA112/SPA122 Analog Telephone Adapter Firmware Release 1.4(1)SR5

First Published: November 4, 2019

Introduction

This document describes describe the updates and fixes in Cisco Small Business SPA112/SPA122 ATA Firmware Release 1.4(1)SR5.

IMPORTANT

As with any firmware release, read these release notes before you upgrade the firmware. We also recommend that you back up the configuration before you perform any firmware upgrade.

Cisco Systems, Inc.
https://www.cisco.com

Hardware and Firmware Compatibility

The following matrix describes the hardware and firmware compatibility.

SPA112, SPA122 (2 types of devices)	Model	SN Range	1.4.1SR5, 1.4.1SR4, 1.4.1SR3, 1.4.1SR1 and 1.4.1(SPA112/SPA122) 1.4.0 (SPA112/SPA122) 1.3.5p and 1.3.2p (SPA112/SPA122)	1.3.5, 1.3.4, 1.3.3, 1.3.2n	1.3.2 or earlier
Device 1 (128MB Flash + New SLIC)	SPA112	CCQ18400001 to CCQ1841033K After CCQ18500DAE	Yes	No	No
	SPA122	CCQ1834031U to CCQ1834037D CCQ1847066I to CCQ184707YA CCQ184902ED to CCQ184904UL CCQ184904UM to CCQ184904Y3 CCQ184904Y4 to CCQ184904Y5 After CCQ185001YH			
Device 2 (128MB Flash + Old SLIC)	SPA112	CCQ175106J3 to CCQ175106OM CCQ181607OO to CCQ181607U7 CCQ18240E34 to CCQ18400000 CCQ1841033L to CCQ18500D9K	Yes	Yes	No
	SPA122	CCQ174602V3 to CCQ1746030M CCQ181502B7 to CCQ181502GQ CCQ182002W3 to CCQ1834031T CCQ1834037E to CCQ18470660 CCQ184707YB to CCQ184902EC CCQ184904UM to CCQ184904UL CCQ184904Y4 to CCQ184904Y3 CCQ184904Y6 to CCQ185001YH			
Device 3 (32MB Flash + Old SLIC)	SPA112	Before CCQ182002W2	Yes	Yes	Yes
	SPA122	Before CCQ181805KR			

Note Do not upgrade any device to an unsupported firmware version as detailed in the Hardware and Firmware Compatibility Matrix table.

Note New SLIC devices have a label that reads *S/W: Must use 1.3.5(004p) or later.*

Upgrade the Firmware

Follow these instructions to upgrade the phone adapter.

Step 1 Download the latest firmware by using the Firmware link on the following web page:

https://www.cisco.com/c/en/us/products/unified-communications/small-business-voice-gateways-ata/index.html

Step 2 Access the adapter Configuration Utility in one of the following two ways:

- If the adapter is SPA112, connect one analog phone to its FXS port, press ***# to access IVR, enter 110 to get SPA112 WAN IP address. Then, launch a web browser, and enter WAN IP address.
- If the adapter is SPA122, connect one PC to its LAN port. Then, launch a web browser, and enter the LAN IP address. The default value is 192.168.15.1.

Step 3 Log in to the Configuration Utility.

Step 4 Click **Administration** in the menu bar, and then click **Firmware Upgrade** in the navigation tree.

Step 5 Click **Browse** and select the location of the upgrade file that you downloaded.

Step 6 Click the **Upgrade** button to upgrade the firmware.

Note Upgrading the firmware may take several minutes. Until the process is complete, do not turn off the power, press the hardware reset button, or click the **Back** button in your current browser.

New and Changed Feature

There are no new or changed features in this release.

Caveats

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

Access Cisco Bug Search

Known problems (bugs) are graded according to severity level. These release notes contain descriptions of the following:

- All severity level 1 or 2 bugs
- Significant severity level 3 bugs

You can search for problems by using the Cisco Bug Search.

Before You Begin

To access Cisco Bug Search, you need the following items:

- Internet connection

- Web browser
- Cisco.com user ID and password

Procedure

Step 1 To access the Cisco Bug Search, go to:

https://tools.cisco.com/bugsearch

Step 2 Log in with your Cisco.com user ID and password.

Step 3 To look for information about a specific problem, enter the bug ID number in the Search for field, then press **Enter**.

Open Caveats

The following table lists severity 1, 2, and 3 defects that are open for the Cisco Small Business SPA112/SPA122 Analog Telephone Adapter Firmware Release 1.4(1)SR5.

For more information about an individual defect, search for the caveat in the Bug Search Toolkit. 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 Access Cisco Bug Search, page 3.

Identifier	Description
CSCvf45915	SPA112/122: Downgrade Rev Limit not recognize SR version
CSCvf53408	SPA112 IVR should not have option 210 LAN IP address
CSCvq50550	Cisco SPA 100 Series Phone Adapters Predictable Authentication Session Keys

Resolved Caveats

The following table lists severity 1, 2, and 3 defects that are resolved for the Cisco Small Business SPA112/SPA122 Analog Telephone Adapter Firmware Release 1.4(1)SR5.

For more information about an individual defect, search for the caveat in the Bug Search Toolkit. 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 resolved at the time this report was compiled. For an updated view of resolved defects, access Bug Toolkit as described in Access Cisco Bug Search, page 3.

Identifier	Description
CSCvq28001	Evaluation SPA112/122 for TCP_SACK
CSCvq46598	Multiple vulnerabilities reported on SPA112 and SPA122
CSCvq50494	Cisco SPA100 Series Analog Telephone Adapters Remote Code Execution Vulnerabilities
CSCvq50503	Cisco SPA100 Series Web-Based Management Interface File Disclosure Vulnerability

Identifier	Description
CSCvq50512	Cisco SPA100 Series Analog Telephone Adapters Reflected Cross-Site Scripting Vulnerability
CSCvq50517	Cisco SPA122 ATA with Router Devices DHCP Services Cross-Site Scripting Vulnerability
CSCvq50520	Cisco SPA100 Series Administrative Credentials Information Disclosure Vulnerability
CSCvq50523	Cisco SPA100 Series Running Configuration Information Disclosure Vulnerability
CSCvq50529	Cisco SPA100 Series Web Management Interface Denial of Service Vulnerability
CSCvq50541	VLAN Protocol Info Stack Overflow
CSCvq50548	Multicast Pass Multiple Stack Overflows
CSCvq79227	SPA112/122 CVE-2019-3896 Linux Kernel dr_remove_all() Function Double-Free Arbitrary Code Exe

Behavior During Times of Network Congestion

Anything that degrades network performance can affect voice and video quality, 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

To reduce or eliminate any adverse effects to the devices, schedule administrative network tasks during a time when the devices are not being used or exclude the devices from testing.

Related Documentation

Cisco Small Business

For more information on Cisco Small Business, see https://www.cisco.com/smb.

Additional Information

For more information on Cisco Small Business Support Community, see https://supportforums.cisco.com/community/5541/small-business-support-community.

For more information on Cisco Small Business Support and Resources, see https://supportforums.cisco.com/community/3226/small-business-support-service.

To access the Phone Support Contacts, see https://www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html.

For downloading the software, see https://software.cisco.com/download/navigator.html.

For more information on Cisco Small Business Voice Gateways Documentation, see https://www.cisco.com/c/en/us/products/unified-communications/small-business-voice-gateways-ata/index.html