Release Notes for Cisco Small Business SPA30X, SPA50X, and SPA51X IP Phone Firmware Release 7.6(2)SR6

First Published: October 31, 2019

Introduction

This document describes the updates and fixes in Cisco Small Business SPA30X, SPA50X, and SPA51X IP Phone Firmware Release 7.6(2)SR6.

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.

Before You Upgrade

When you upgrade a Cisco SPA50X or Cisco SPA30X IP Phone that is running a release prior to 7.5.2b, you must first upgrade to 7.5.2b before you upgrade to a later release. See the following table for more information.

Firmware Release Installed on Your Phone	Special Instructions for Upgrading to Release 7.5.3 or Later
7.5.2b or later	None
7.5.1	Upgrade to 7.5.2b first, then upgrade to 7.5.3 or later.
7.4.x	
7.3.x	

Software Compatibility

Firmware Release 7.6(2)SR6 includes all customer-found defects that have been fixed after Firmware Release 7.6(2)SR5. For SPA5x5, the openssl library upgrades to openssl-0.9.8zh.

New and Changed Features

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

There are currently no open defects for the Cisco Small Business SPA30X, SPA50X, and SPA51X for Firmware Release 7.6(2)SR6.

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 2.

Resolved Caveats

The following table lists severity 1, 2, and 3 defects that are resolved for the Cisco Small Business SPA30X, SPA50X, and SPA51X for Firmware Release 7.6(2)SR6.

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 2.

Identifier	Headline
CSCvn17128	SPA5x5: TLS connection opened to ANY SIPs server, regardless of issuing CA of its certificate.
CSCvn53399	Cisco SPA50x/51X phones dropping calls When Caller ID is the same
CSCvp59831	SPA504G, SPA303: does not send PIN DTMF randomly
CSCvp76917	SPA514G fails to perform the SSL re-negotiation
CSCvp79024	SPA514G delay caused by excessive certification negotiation
CSCvr64019	SPA508G Stops generating RTP after a certain period of time
CSCvr64010	SPA508G Stops generating RTP within 5 minutes

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.

Cisco Small Business Product Documentation

For more information on Cisco Small Business SPA500 Series IP Phones, see https://www.cisco.com/c/en/us/products/collaboration-endpoints/small-business-spa500-series-ip-phones/index.html.

For more information on Regulatory Compliance and Safety Information for the Cisco SPA300 Series and Cisco SPA500 Series IP Phones, see

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/csbpipp/ip_phones/regulatory_compliance/guide/rcsi_SPA300_SPA500.pdf.

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, see https://supportforums.cisco.com/community/3226/small-business-support-service.

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