Release Notes for Cisco Small Business SPA30X, SPA50X, and SPA51X IP Phone Firmware Release 7.6(2)SR1

First Published: December 12, 2016

Introduction

This document describes the updates and fixes in Cisco Small Business SPA30X, SPA50X, and SPA51X IP Phone Firmware Release 7.6(2)SR1.

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	

Cisco Systems, Inc.
www.cisco.com

Software Compatibility

Firmware Release 7.6(2)SR1 includes all customer-found defects that have been fixed after firmware release 7.6.2. For SPA5x5, the openssl 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

The following table lists severity 1, 2, and 3 defects that are open for the Cisco Small Business SPA30X, SPA50X, and SPA51X for Firmware Release 7.6(2)SR1.

For more information about an individual defect, search for the caveat in the Bug Search Tookit.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 2.

Identifier	Headline
CSCvb27688	VxWorks DHCP and DNS Vulnerabilities - SPA300 - SPA500 (need vendor)
CSCvb91638	SPA514G: Large directory delay due to large certificates
CSCvb93595	SPA514G SR=680504966: DTMF not sent Inband when Inband is negotiated
CSCvc29455	SPA50x kem_status shows the KEM was enabled but it is offline actually

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)SR1.

For more information about an individual defect, search for the caveat in the Bug Search Tookit.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 2.

Identifier	Headline
CSCuz76576	SPA508G: Intermittently KEM module locks up after sidecar unplug message
CSCuz91356	Cisco Small Business SPA3x/5x series CSRF remote arbitrary fw load vuln
CSCvb27334	SPA5xx - Change in fw upgrade and downgrade memory allocation mechanism
CSCvc11839	SPA50X SR=639206733:Issue with the caller ID showing up not complete,CALL ID display length revert
CSCvc21113	SPA5xx enlarge the code size limitation to adapt to the size on flash

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 http://www.cisco.com/smb.

Cisco Small Business Product Documentation

For more information on Cisco Small Business SPA500 Series IP Phones, see http://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

http://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 documents, see https://software.cisco.com/download/navigator.html.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

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. (1110R)

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.

© 2016 Cisco Systems, Inc. All rights reserved.