Field Notice: FN - 72352 - SPA5xx: QuoVadis Root CA 2 Decommission Might Affect SIP and HTTPS handshake - Product

Notice

THIS FIELD NOTICE IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTY OF MERCHANTABILITY. YOUR USE OF THE INFORMATION ON THE FIELD NOTICE OR MATERIALS LINKED FROM THE FIELD NOTICE IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS FIELD NOTICE AT ANY TIME.

Revision History

Revision	Publish Date	Comments
1.0	01-Mar-22	Initial Release

Products Affected

Affected Product ID	Comments
SPA500DS	
SPA508G	
SPA509G-RC	
SPA504G-XU	
SPA512G	
SPA502G-XU	
SPA509G	
SPA525G2	
SPA502G	
SPA500S	
SPA504G	

Defect Information

Defect ID	Headline

CSCvx00508	QuoVadis root CA decommission on spa5x5

Problem Description

For affected versions of the SPA500 series phone, some Secure Sockets Layer (SSL) certificates issued from the QuoVadis root certificate authority (CA) trust chain before March 31, 2021 cannot be renewed from this CA. Once those certificates expire on devices or are removed from the Cisco cloud servers, functions such as SIP and HTTPS connections will fail to establish.

Background

The QuoVadis Root CA 2 Public Key Infrastructure (PKI) used by SPA500 series phones to issue SSL certificates is subject to an industry-wide issue that affects revocation abilities. Due to this issue, no new QuoVadis Root CA 2 certificates will be issued or renewed by Cisco after March 31, 2021. This affects certificate renewals on devices, Cisco cloud servers, and third-party services.
Certificates issued before the QuoVadis Root CA 2 was decommissioned will continue to be valid. However, the certificates will not renew when they expire on either the device or the Cisco cloud server. This will cause functions such as SIP and HTTPS connections to fail to establish.

Problem Symptom

Expiration of the QuoVadis Root CA 2 certificates affects SIP or HTTPS communications and will cause handshakes to fail. Phones may not be provisioned and/or negotiate SIP security, and other security related features (not SIP related) may not work.

Workaround/Solution

Cisco has migrated from the QuoVadis Root CA 2 to the IdenTrust Commercial Root CA 1 for SSL certificates.

Unfortunately there is no workaround and no software upgrade available due to the end of software support (see EOL notice13284). Cisco recommends migration to a device that is supported. The Cisco account team or reseller can help to understand what kind of options are available.

For More Information

Cisco has created a web page to provide customers and partners with additional information on this issue. Consult the QuoVadis Root CA 2 Decommission page for a full list of products affected, associated Field Notices, and frequently asked questions.

If you require further assistance, or if you have any further questions regarding this field notice, please contact the Cisco Systems Technical Assistance Center (TAC) by one of the following methods:

- Open a service request on Cisco.com
- By email or telephone

Receive Email Notification For New Field Notices

My Notifications—Set up a profile to receive email updates about reliability, safety, network security, and end-of-sale issues for the Cisco products you specify.