Cisco Expressway SHA-1 Certificate Deprecation Rollout and SHA-2 Certificate Transition

First Published: November 2024

Important change announcement - deprecation of SHA-1

Background

SHA-1 (Secure Hash Algorithm 1) is widely used for digital certificates. However, it is now considered insecure due to vulnerabilities that allow collision attacks. As a result, many industry standards and security policies have deprecated SHA-1 in favor of SHA-2 (Secure Hash Algorithm 2) algorithms. TLS 1.3, the latest Transport Layer Security protocol version, mandates strong cryptographic algorithms, further necessitating the transition from SHA-1.

Purpose

The purpose is as follows:

- Explain the changes in Cisco Expressway X15.2, specifically regarding SHA-1 certificates.
- Describe the impact on new installations and upgrades.
- Guides transitioning to SHA-2 signed certificates.
- Detail the scenarios where SHA-1 signed certificates are still accepted.

SHA-1 Deprecation and TLS 1.3

Support Rationale Security Vulnerabilities

SHA-1 is vulnerable to collision attacks, where two different inputs produce the same hash output. Hackers exploit this to forge digital certificates, compromising the security of encrypted communications.

Industry Standards

Regulatory bodies and industry standards, including the Internet Engineering Task Force (IETF) and the National Institute of Standards and Technology (NIST), have deprecated SHA-1. Major browsers and certificate authorities have also phased out support for SHA-1 signed certificates.

TLS 1.3 Requirements

TLS 1.3 requires the use of strong cryptographic algorithms and does not support SHA-1. Supporting TLS 1.3 necessitates using SHA-2 signed certificates for secure communications, particularly for internal components like clustering.

Impact on Cisco Expressway Deployments

Certificate Upload Restrictions

Going forward, Users cannot upload server certificates signed with the SHA-1 algorithm if the Cisco Expressway version is X15.2 and beyond. This applies to both new installations and upgrades. However, Expressway, as a client, will continue to accept SHA-1-signed certificates to ensure backward compatibility.

Deployment Scenarios

Fresh Installations

For new installations of Cisco Expressway X15.2:

1. **Obtain SHA-2 Signed Certificates:** Ensure server certificates are signed with the SHA-2 algorithm (e.g., SHA-256).
2. **Upload Certificates:** Upload the SHA-2 signed certificates to the Expressway system during installation.
3. **Verify Configuration:** Confirm that the certificates are correctly installed and that all communications are secure.

Upgrades from Previous Versions

For upgrades from versions before X15.2:

1. **Pre-Upgrade Check:** Verify the current server certificates. If signed with the SHA-1 algorithm, proceed with the following steps before upgrading.
2. **Obtain SHA-2 Signed Certificates:** Contact your certificate authority (CA) to obtain new certificates signed with the SHA-2 algorithm.
3. **Update Certificates:** Upload the new SHA-2 signed certificates to the Expressway system.
4. **Perform Upgrade:** Proceed with the upgrade to version X15.2. The upgrade will fail if SHA-1 signed certificates are still in use.

Handling SHA-1 Signed Certificates

Expressway as a Client

While Expressway X15.2 will not allow the upload of SHA-1-signed server certificates, it will continue to accept SHA-1-signed certificates when acting as a client. This ensures compatibility with external systems and certificates that have not yet transitioned to SHA-2.

Transition Guidelines

Obtaining SHA-2 Signed Certificates

1. **Contact Certificate Authority (CA):** Contact your CA to request certificates signed with the SHA-2 algorithm.

2. **Specify Requirements:** Ensure the request specifies SHA-256 or a stronger SHA-2 variant.

3. **Download Certificates:** Once issued, download the new certificates and the complete certificate chain (root and intermediate certificates).

Installing SHA-2 Signed Certificates

On Expressway-E

1. **Access Admin Interface:** Open the Expressway-E administrative interface and log in with administrative credentials.

2. **Upload Server Certificate:** Navigate to Maintenance -> Security -> Server Certificate and upload the new SHA-2-signed server certificate.

3. **Update Trusted CA List:** Ensure that the root and intermediate CA certificates for the SHA-2 chain are present. Upload any missing CA certificates.

4. **Restart:** Restart the Expressway-E to apply the new certificates.

On Expressway-C

1. **Access Admin Interface:** Open the Expressway-C administrative interface and log in with administrative credentials.

2. **Upload Server Certificate:** Navigate to Maintenance -> Security -> Server Certificate and upload the new SHA-2-signed server certificate.

3. **Update Trusted CA List:** Ensure that the root and intermediate CA certificates for the SHA-2 chain are present. Upload any missing CA certificates.

4. **Restart:** Restart the Expressway-C to apply the new certificates.

Testing and Validation

1. **Verify Certificate Installation:** Confirm that the new SHA-2-signed certificates are correctly installed on Expressway-E and Expressway-C.

2. **Test Secure Communications:** Conduct tests to ensure that all secure communications, including MRA and clustering, function correctly.

3. **Monitor Logs:** Check the system logs for any errors or warnings related to certificate validation and secure communications.

Conclusion

The transition from SHA-1 to SHA-2 signed certificates in Cisco Expressway X15.2 is critical in enhancing security and supporting TLS 1.3. Please follow the guidelines outlined in this whitepaper to ensure a smooth transition and maintain secure communications. The continued acceptance of SHA-1 signed certificates when Expressway acts as a client ensures compatibility with existing systems during this transition period.

> **Note**: Cisco Expressway X15.2 allows uploading the SHA-1 signed certificate. If the system administrator uploads the SHA-1 signed certificate, it will impact Expressway's clustering. Future releases of Expressway will not allow users to upload a SHA-1 signed certificate.

References

- NIST Special Publication 800-57, " Recommendation for Key Management - Part 1: General"
- IETF RFC 6194, " Deprecation of SHA-1 in Internet Protocols"

Summary

This document details the rationale behind SHA-1 Certificate Deprecation and its impact on various deployment scenarios. It also provides guidelines for ensuring a smooth transition to SHA-2-signed certificates.

Going forward, users cannot upload server certificates signed with the SHA-1 algorithm if the Cisco Expressway version is X15.2 or later. However, Expressway will still accept SHA-1-signed certificates as a client. This change aligns with industry standards for enhanced security and supports the introduction of TLS 1.3, which requires stronger cryptographic algorithms.

Documentation Changes

Table 2. Documentation Changes

Date	Change
October 2024	Published the whitepaper for SHA-1 Certificate.

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*.

You can subscribe to the What's New in the Cisco Product Documentation RSS feed to receive new and revised Cisco technical content directly to your desktop. The RSS feeds are a free service.

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 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 are considered un-Controlled copies, and the original on-line version should be referred to for 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)