Cisco Voice over IP (VoIP) Compliance for the Payment Card Industry (PCI)

What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards devised to safeguard all companies that accept, obtain, process, save, or transmit credit card information. It applies to organizations of all sizes with any number of online transactions that accept, pass on, or store cardholder information. This could be over the phone, Internet, or any other means.

Who is affected by PCI DSS?

PCI DSS applies to all entities that engage in card processing, including merchants, processors, acquirers, issuers, and payment service providers. PCI DSS also applies to all entities that store, process, or transmit Cardholder Data (CHD) and Sensitive Authentication Data (SAD).

Benefits

Types of VoIP traffic affected by the Payment Card Industry Data Security Standard (PCI DSS):

- VoIP traffic that contains payment card account data
- Call recording management and storage
- Control of the agent or caller interface within the physical call-center space

Learn more

About upgrading your phone security to TLS 1.2 to be compliant with PCI today.

If an organization is found to be non-compliant, it could be fined anywhere between $5000 and $100,000 U.S. dollars per month. These violations could also incur huge card replacement costs and in-depth investigations into the business. For more details on security and compliance, visit Cisco.com/go/voipcompliance.

C45-742607-00 07/19

Recommendations

The PCI DSS Council considers strong encryption to be a security best practice. It recommends the use of TLS 1.2. SSL and TLS (1.0) are not allowed under PCI DSS v3.2.

Cisco collaboration secured architecture

Cisco is committed to a strong focus on security beyond PCI DSS compliance. You can find more details about Cisco Collaboration Secured Architecture at Cisco Preferred Architectures.

Cisco collaboration software

To support TLS 1.2, administrators should update the collaboration environment to software release 11.5.1 (SU3), and contact center software to release 11.6(1) for the relevant following applications:

- Cisco® Unified Communications Manager
- Cisco Unified Contact Center Enterprise solutions
- Cisco Unified Contact Center Express solutions
- Cisco Customer Journey Platform
- IM and Presence
- Cisco Unity® Connection
- Cisco Prime® Collaboration Deployment for releases earlier than 11.5.1 (SU3)

Cisco voice endpoints

Legacy Cisco IP phones

Replace any legacy Cisco IP phones (6900, 7900, 8900, and 9900 Series) with newer models such as the 7800 or 8800 Series. The 7800 and 8800 Series phones support TLS 1.2. For more information, see the Cisco Endpoints portfolio page.

Cisco IP Phone 7800 Series and 8800 Series

Cisco IP Phone 7800 Series and 8800 Series should be upgraded with firmware release 12.1 in order to support TLS 1.2.

For more details on security improvements in the latest Cisco IP phones, refer to the Cisco IP Phone 7800 and 8800 Series Security Overview.

Cisco video endpoints

Legacy Cisco TelePresence

Newer TANDBERG™ Codec (TC) endpoints support collaboration endpoint software (CE) release 9.1(3).

For legacy TC endpoints, such as C-Series, EX, MX200 or MX300 G1, or Profile, consider upgrading to Cisco TelePresence® TC software release 7.3(11).

Legacy immersive systems such as the TX9000 series and Cisco TelePresence System will not support TLS 1.2.

Cisco collaboration endpoint software

Consider upgrading any CE endpoints (Cisco DX70 or DX80 or Cisco TelePresence MX200 or MX300 G2, MX700 or MX800, or SX Series) to Cisco CE software release 9.1(3).

*Note: Cisco DX650 endpoints on Android should be replaced with newer hardware.