Cisco Voice over IP (VoIP) Readiness for the General Data Protection Regulation (GDPR)

How does GDPR apply to VoIP?

Awareness of privacy and data protection issues among customers, employees, partners, policy makers, and the media has significantly increased over the last couple of years. The general catalysts have been data breaches and mishandling of data, along with regulatory reform such as the EU's General Data Protection Regulation (GDPR), which imposes significant financial penalties (up to four percent of annual gross revenue).

Using state-of-the-art technology to lower the applicable and assessed risk of processing of personal data is recommended because it allows you to keep up to date with recommendations from leading industry groups, technical subject matter experts, and vendors.

Concerning TLS version support, the Internet Engineering Task Force (IETF) clearly states in section 4 of its draft memo,[1] **"Deprecating TLSv1.0 and TLSv1.1"**:

"TLSv1.0 MUST NOT be used. Negotiation of TLSv1.0 from any version of TLS MUST NOT be permitted. Any version of TLS is more secure than TLSv1.0 and can be configured to prevent interception..."

Further to this, the German Federal Office for Information Security states in one of its Technical Guidelines[2] that **"...in general, TLS 1.2 or TLS 1.3 should be used, and that TLS 1.0 and TLS 1.1 are not recommended."**

In this context, the collaboration environment, including software, voice endpoints, and video endpoints, should be updated to support TLS 1.2.

Personal data inherent to VoIP calls

IP phone calls that are not properly secured can expose an individual's personal data, including:

- The content of the voice conversation
- Identification of the entities involved in the call, such as phone numbers and URLs
- Call history, including frequency and duration of calls
- Missed calls and transfers

Learn more

About upgrading your phone security to support TLS 1.2 to be GDPR ready today.

Violations on certain articles of GDPR carry fines of up to €20 million or up to four percent of an organization's total global revenue from the preceding year, whichever is greater. For more details on security and compliance, visit Cisco.com/go/voipcompliance.

C45-742606-00 07/19

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

The 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 systems

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

For legacy TC endpoints, such as the 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 (CE) software

Consider upgrading any CE endpoints (including the 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.