Cisco Response to NCSC “Video conferencing services: security guidance for organisations”

In April 2020 the NCSC published security guidance aimed at public and private sector organisations for video conferencing services. The new guide builds on top of the already published SaaS security guidance and Cloud Security Principles, adding in specific areas of consideration for Video Conferencing applications.

This document provides a response to the new guidance for the Cisco Webex Meetings platform. It covers specific sections for how Webex meets the SaaS security principles and the video conferencing specific considerations. A separate document has been produced which describes how the Webex Meetings platform meets the main NCSC Cloud Security Principles.

Cisco Webex Meetings Overview

Cisco Webex Meetings is a cloud-based web and video conferencing solution that enables global employees and virtual teams to collaborate in real time from anywhere, anytime, on mobile devices or video systems as though they were working in the same room. Solutions include meetings, events, training, and support services.

Cisco Webex is a Software-as-a-Service (SaaS) solution delivered through the Cisco Webex Cloud, a highly secure service-delivery platform with industry-leading performance, integration, flexibility, scalability, and availability. The Cisco Webex Cloud is a communications infrastructure purpose-built for real-time web communications. Cisco Webex meeting sessions use switching equipment located in multiple data centres around the world. These data centres are strategically placed near major Internet access points and use dedicated high-bandwidth fibre to route traffic around the world. Cisco operates the entire infrastructure within the Cisco Webex Cloud with industry-standard enterprise security.

Cisco Webex Industry Standards and Certifications

In addition to complying with our stringent internal standards, Cisco Webex also continually maintains third-party validations to demonstrate our commitment to information security. Cisco Webex maintains the following industry standard certifications:

- ISO/IEC 27001:2013, 27017:2015, and 27018:2019
- Service Organization Controls (SOC) 2 Type II
- FedRAMP certified (visit cisco.com/go/fedramp for more details, scope, and availability) Note: FedRAMP certified Webex service is only available to U.S government and education customers
- Cloud Computing Compliance Controls Catalogue (C5)
- Privacy Shield Framework

Cisco Webex and the NCSC Cloud Security Principles

Due to the extensive nature of the NCSC Cloud Security Principles and the associated responses, the assessment of Cisco Webex Meetings against the principles is contained in a separate document.

Cisco Webex and NCSC SaaS Security Principles

The table below outlines the Cisco Webex response to each of the NCSC SaaS Security Principles. Additional detail can be found at:

https://trustportal.cisco.com/c/r/ctp/trust-portal.html#/customer_transparency

https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf

PRINCIPLE	CISCO RESPONSE
Data-in-transit protection between clients and the service	**Encryption at run time** All communications between Cisco Webex applications and Cisco Webex Cloud occur over encrypted channels. Cisco Webex uses TLS 1.2 protocol with high strength cipher suites. The current list of offered cipher suites is included in the Cisco Webex Meetings Security Whitepaper After a session is established over TLS, all media streams (audio VoIP, video, screen share, and document share) are encrypted.[2] Encrypted media can be transported over UDP, TCP or TLS, User Datagram Protocol (UDP) is the preferred transport protocol for media. Media packets are encrypted using either AES 128 or AES 256. Webex Video devices and 3rd party video devices that support media encryption with SRTP use AES-GCM-128-HMAC-SHA1. Webex Applications use AES-GCM-256.[1] The initial key exchange occurs over a TLS-secured channel. **End-to-end encryption** For standard meetings, servers may need to decrypt for PSTN, transcoding and recording. However, for customers requiring a higher level of security, Cisco Webex also provides end-to-end encryption. With this option, Cisco Webex Cloud does not have access to the encryption keys used by meeting participants and cannot decrypt the media streams. With end-to-end encryption, the meeting encryption key is generated by the meeting host and securely distributed to all other participants in the meeting. To secure the meeting encryption key prior to transmitting it via the Webex cloud to each meeting participant, the key is encrypted by the meeting host. To achieve this, each Cisco Webex client generate 2048-bit RSA public and private key pairs and sends the public key to the meeting host's client. The host encrypts the meeting key using the public key that the client sends and returns the encrypted meeting encryption key back to the client. The client can then decrypt the meeting key using its RSA private key. All meeting data (voice, video, chat etc.) generated by Cisco Webex clients is encrypted using the shared meeting encryption key. Using Webex End to End Encryption meeting data cannot be deciphered by Cisco Webex service. This end-to-end encryption option is available for Cisco Webex Meetings and Cisco Webex Support. Note that when end-to-end encryption is enabled, the following features are not supported: ▪ Personal Room meetings ▪ Join Before Host ▪ Video-device enabled meetings ▪ Cisco Webex Meetings Web App ▪ Linux clients ▪ Network-Based Recording (NBR) ▪ Saving session data, Transcripts, Meeting Notes, and etc... ▪ Remote Computer sharing

[1] Support for Webex Applications using AES-256-GCM for media encryption is being rolled out, starting June 2020.

[2] Users connecting to a cloud meeting using a third-party video endpoint may be sending and receiving unencrypted media streams. Configuring your firewall to prevent unencrypted traffic to and from Cisco Webex helps keep your meetings safe. However, allowing attendees outside your firewall to join your meeting using third-party devices can still send your meeting data unencrypted on the Internet.

PRINCIPLE	CISCO RESPONSE
Industry good practice external certificate configuration	Certificates are issued from a well-known public PKI (Quovardis) Certificates are issued with a 1 year lifetime Certificates use RSA 2048-bit keys Strict Transport Security (HSTS) is enabled
Data-in-transit protection between microservices	The Webex Meetings platform operates on a global, private network and sensitive data which is transferred between data centres is protected in transit.
Industry good practice internal certificate configuration	Where certificates are used for internal authentication they follow industry good practice configuration.
API authentication and protection	The Webex platform offers a REST API for external application integration. Access to the API is protected by an access token which is passed in the HTTP 'Authorization' header field. Data exchanged via the API is protected using TLS 1.2.
Privilege separation	Webex Meetings is built around five distinct roles with a defined set of permissions; Host, Alternate Host, Presenter, Panellist, Attendee and Site Administrator.
Multi-factor authentication	Cisco Webex supports the use of single-sign on (SSO) using the SAML 2.0 protocol. This protocol allows integration with third-party identity solutions such as Duo, PingFederate, OpenAM or Microsoft Active Director Federation Services. In addition to SSO via SAML, WebEx administrators can set a range of options for standard user passwords such as password aging, complexity, password blacklists etc.
Logging and event collection	Cisco Webex has implemented key operational metrics and alarms across the production network using a variety of automated monitoring systems to detect outages, service latency, security incidents and other unusual or unauthorised activities and events. Alarms are configured to notify operational and management personnel when warning thresholds are met, indicating potential service latency, server unavailability, or other factors affecting availability and functionality. Cisco policy establishes the requirements for logging data, which includes requirements for event types, time synchronisation, content and other key information. Logs are centralised for aggregation, correlation, continuity and retention.
Availability of logs	Webex Meetings captures administrative audit logs within its native management console and makes these available to the customer. These logs contain detailed information regarding changes to the site configuration and can be exported in CSV format.

PRINCIPLE	CISCO RESPONSE
Clear incident response to patching and security issues	The Cisco Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation and public reporting of security vulnerability information related to Cisco products and networks. PSIRT maintain a comprehensive security vulnerability policy which is available online at https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html Patches are prioritised per the Webex change management process. Patches are developed, tested and reviewed and approved by the Change Approval Board before incorporated into the release cycle either as an emergency patch or scheduled in a future release cycle. Patch timelines are derived based on the vulnerability's severity (in accordance with CVSS scoring thresholds).
Clear and transparent details on a product's security features	https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf https://trustportal.cisco.com/c/r/ctp/trust-portal.html?solutioncategory=Collaboration https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-742369.html

Cisco Webex and the NCSC Video Conferencing Guidance

As outlined in the introduction to this document, the NCSC Video Conferencing guidance builds on top of the already established SaaS and cloud security principles. The additional areas that are specific called out in the guidance include:

PRINCIPLE	CISCO RESPONSE
Request copies of independent assessments or audits	The WebEx Meetings platform has undergone numerous external assessments including ISO 27001:2013 and SOC 2. Additionally, Cisco publishes both a Privacy Data Sheet and Privacy Data Map which includes extensive details regarding the processing of personal data within the Webex Meetings platform. All documents can be found on the Cisco Trust Portal at https://trustportal.cisco.com/c/r/ctp/trust-portal.html?search_keyword=webex%20meetings Terms and Conditions for the Webex service are covered by Cisco's Universal Cloud Agreement which can be found at https://www.cisco.com/c/en/us/about/legal/cloud-and-software/universal-cloud-agreement.html Supplemental terms are included in the Webex Offer Description which is available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/cisco_webex_offer_description.pdf
Data Centre Jurisdictions	The Webex Meetings service leverages its own data centres which are located across the globe. The exact locations are outlined in the Privacy Data Sheet. User-Generated Information is stored in the data centre closest to a Customer's location or as provided during the ordering process. Billing data is stored in Texas, USA and North Carolina, USA. Webex Analytics data is stored in California, USA and Texas, USA. User-generated information is defined as: • Meeting and Call Recordings • Transcriptions of Call Recordings • Uploaded Files (for Webex Events and Training only)
Single-Sign On Integration	As described in the response to the SaaS Security principles, Webex Meetings supports SAML 2.0 which can be used to integrate into a range of existing identity solutions to deliver single-sign on to the service.
Ability to control access to meetings	Webex Meetings provides a wide range of control over access to meetings. Full guidance is available in the documentation at https://help.webex.com/en-us/8zi8tq/Cisco-Webex-Best-Practices-for-Secure-Meetings-Hosts Addressing the points specifically called out in the NCSC Guidance: • Webex Meetings can be configured to allows users within an organisation to join a meeting directly. • Webex can be configured to enforce a meeting password for External meeting participants. Participants will need to provide the password prior to being able to join the meeting. • Lobby use within WebEx is configurable and can set such that external, unauthenticated participants can be placed into a lobby such that the meeting host has to manually admit them. In addition to the above, all meetings can be manually locked by the host, or automatically after a configurable time after the meeting has started. Once locked, access to the meeting is blocked for all users and they will be entered into the lobby where the host can then admit them.

PRINCIPLE	CISCO RESPONSE
Additional Meeting Features	The NCSC guidance highlights that many conferencing solutions offer additional features that customers should be aware of. The Webex service offers all of the capabilities outlined in the guidance, i.e. • File sharing • Screen sharing • Instant Messaging Chat • Call transcription • Remote desktop control
Call recordings and shared files	As noted above, these files are considered User-Generated information and if the necessary features are enabled, will be stored in data centre closest to the customer's location or as provided during the ordering process.