CSB
CYBER SECURITY BRUNEI

contact@csb.gov.bn
(673) 245 8002
Simpang 69, Jalan E-Kerajaan
Gadong BE1110, Negara Brunei Darussalam
www.csb.gov.bn

SECURITY GUIDELINES ON USING ONLINE COLLABORATION TOOL *CISCO WEBEX*

9 August 2021

DOCUMENT CHANGE HISTORY

Version	Date	Change Description
1.00	*2/3/2021*	*Initial draft*
1.10	*9/8/2021*	*Content added*

Table of Contents

INTRODUCTION

Online collaboration provides an organization with a platform to communicate and collaborate entirely, connecting more people and processing more information internally or externally at a quick decision-making rate. The tool can be called into action as a contingency plan when an emergency crisis occurs or it can be part of the organization's modernization, digitization and transformation strategy to innovate the delivery of public services by making its internal processes more efficient and effective. As a result, time is saved, work gets done more quickly and information becomes knowledge which is more easily transferrable across the department and cross sectorial.

However, using collaboration tools online can present security risks to the organization's networks and computing systems. Any organizations embarking for this online business solution are required to refer to their **respective data classification policies** for additional security guidelines in managing and handling organization official classified information specifically and must already put in place an organization-wide **Cloud Policy** as these tools are almost exclusively on the cloud.

The online collaboration tools are getting more sophisticated with a variety of features to suit different groups of people and the users are required to be familiar with the product features, functionalities or configuration and customize them to minimize the security risks prior to using the product for organization's use.

This security guideline shall be revised from time to time or be supplemented with updated advisories and recommendations to further improve the security and minimize the risks to the organization in using online collaboration.

PURPOSE

The purpose of this document is to provide guidelines for the organization to enhance the security environment, features and configuration when using Cisco Webex as the preferred communication and collaboration workspace to address the organization online business solution.

INTENDED AUDIENCE

This document is intended for use by all organization personnel in the organization who are authorized and have been familiar in using the product for official online use.

WHAT IS CISCO WEBEX

Webex by Cisco is an enterprise solution for video and audio conferencing, online meetings, screen sharing, application sharing and webinars. It works across web, desktop, mobile and video systems.

There are several ways to join a Webex meeting; through email invitation, from a meeting link, or with a meeting number (number and password will be provided in the email invitation).

RISKS ASSOCIATED WITH CISCO WEBEX

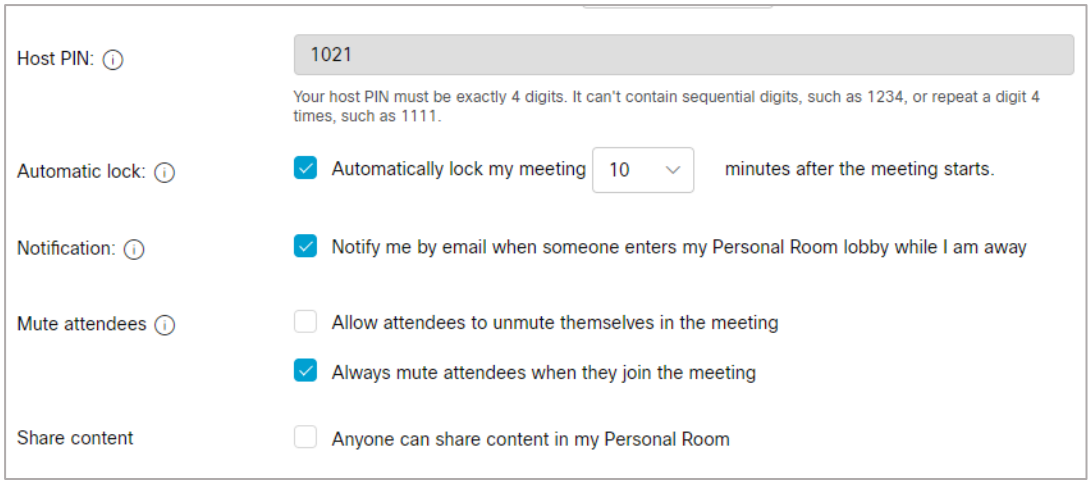
- Anyone with the shared meeting link can join the meeting, so avoid sharing the link on social media unless you want it to be a public event.
- Avoid using your Personal Meeting ID (PMI) to host public events, as it would allow anyone to connect with you even when the event is over.
- Users can record the meeting including its text transcription and any active chats and save it to the cloud where it can be accessed by other users.
- Uninvited people can join the meeting if they have the link.
- Participants list should be checked first to avoid accidentally sharing confidential information.

WEBEX SECURITY CHECKLIST

1. Personal Room Security settings

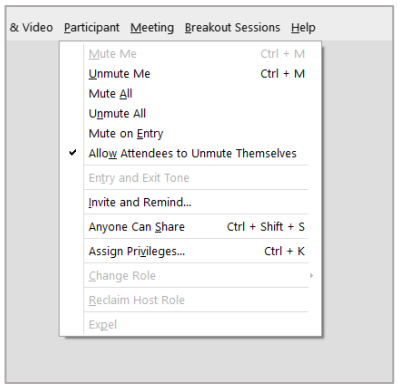
   Edit the settings as below:

   - Automatically lock the Personal Room once attendees have joined the meeting
   - Require attendees to authenticate prior to entering the host's Personal Room (Webex apps and video endpoints)
   - Apply policies for placing authenticated attendees and guests into the lobby, based on whether the meeting is locked or unlocked
   - Allow or disallow attendees to notify the host when they are in the lobby
   - Set lobby timeout values (maximum wait time)
   - Enforce the host PIN length (to be used to enter the Personal Room from a video endpoint)

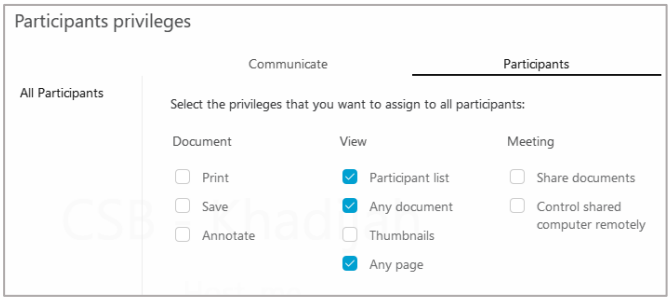


2. <u>Strictly disable sharing options</u>

- Disable or restrict ‘Anyone can share’ to avoid unwanted file sharing

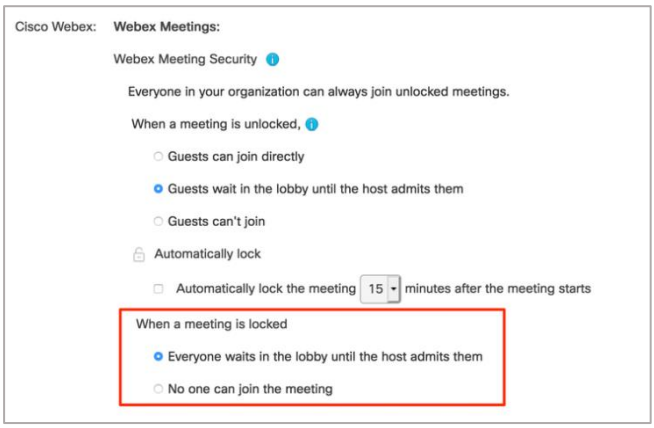


- Assign privileges to participants



3. Virtual Meeting Lobby (Site Administrators)

- Enable the virtual lobby to identify the members before joining the meeting. This will make sure the host can monitor and see everything before other users cause any trouble.



*VULNERABILITIES DISCOVERED

There are several vulnerabilities discovered on Cisco Webex:

Vulnerabilities:

Cisco Webex Meetings Cross-Site Scripting Vulnerability

CVE-ID: CVE-2021-1351

Description:

A vulnerability in the web-based interface of Cisco Webex Meetings could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface of the affected service.

The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected service. An attacker could exploit this vulnerability by persuading a user of the interface to click a maliciously crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.

Impact:

- Arbitrary script code could allow attacker to gain access to sensitive information in web-based interface of Cisco Webex Meetings.

Recommendations:

- Download the latest version of Cisco Webex.
- Make sure to download from trusted resources.

Remarks:

Cisco has confirmed that this vulnerability does not impact Cisco Webex Meeting Server.

* *This issue should be dealt with by CIOs and CTOs*

Vulnerabilities:

Cisco Webex Meetings Desktop App and Webex Productivity Tools for Windows Shared Memory Information Disclosure Vulnerability

CVE-ID: CVE-2021-1372

Description:

Vulnerability in Cisco Webex Meetings Desktop App and Webex Productivity Tools for Windows could allow an authenticated, local attacker to gain access to sensitive information on an affected system.

This vulnerability is due to the unsafe usage of shared memory by the affected software. An attacker with permissions to view system memory could exploit this vulnerability by running an application on the local system that is designed to read shared memory. A successful exploit could allow the attacker to retrieve sensitive information from the shared memory, including usernames, meeting information, or authentication tokens.

Impact:

- Arbitrary script code could allow attacker to gain access to sensitive information on an affected system.

Recommendations:

- Download the latest version of Cisco Webex.
- Make sure to download from trusted resources.

Remarks:

Cisco has confirmed that this vulnerability does not affect the Apple Mac OS X or Linux versions of these products.

GENERAL RECOMENDATIONS

- Download “Cisco Webex” from the creator or a recognized source.
- Update “Cisco Webex” to the latest version as soon as possible.
- Setup password for all online meetings.
- Strict file transfer options.

REFERENCES

- *https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-wda-pt-msh-6LWOcZ5.html#fs*
- *https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-xss-Lz6HbGCt*
- *https://nvd.nist.gov/vuln/detail/CVE-2021-1372*
- *https://nvd.nist.gov/vuln/detail/CVE-2021-1351*
- *https://help.webex.com/en-us/sf4sh1/Webex-Security-Best-Practices#id_134644*