Cisco Security Advisory

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

Medium

Advisory ID:
cisco-sa-wda-pt-msh-6LWOcZ5

First Published:
2021 February 17 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCvv02342 , CSCvv21029

CVE-2021-1372

CWE-202

CVSS Score:
Base 5.5

Download CVRF

Email

Summary

A 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.

Note: To exploit this vulnerability, an attacker must have valid credentials on a Microsoft Windows end-user system and must log in after another user has already authenticated with Webex on the same end-user system.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wda-pt-msh-6LWOcZ5

Affected Products

Vulnerable Products

This vulnerability affects Cisco Webex Meetings Desktop App and Cisco Webex Productivity Tools releases earlier than releases 40.6 and 40.10 when they are running on a Microsoft Windows end-user system.

This vulnerability affects Cisco Webex Meetings Server Desktop App and Cisco Webex Productivity Tools releases that are included with Cisco Webex Meeting Server releases earlier than Release 4.0MR3 SP4 when they are running on a Microsoft Windows end-user system.

For information about which Cisco software releases are vulnerable, see the Fixed Software section of this advisory.

To determine whether a vulnerable release of Cisco Webex Meetings Desktop App is installed on a Windows machine, launch the Cisco Webex Meetings application, click the gear icon in the top right of the application window, and choose the **About...** menu entry. A popup window displaying the currently installed release will open. This is also documented in the article Check the Cisco Webex Meetings Desktop App Version.

To determine whether a vulnerable release of Cisco Webex Productivity Tools is installed on a Windows machine, right-click the Webex Productivity Tools icon on the Windows taskbar and select **About** from the menu. A popup window displaying the currently installed release will open. This is also documented in the article Check the Cisco Webex Productivity Tools Version for Windows.

Products Confirmed Not Vulnerable

Only products listed in the Vulnerable Products section of this advisory are known to be affected by this vulnerability.

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

Details

Cisco Webex Meetings Desktop App allows easy access to commonly used Webex Meetings controls. With the Cisco Webex Meetings desktop app, you can start and join meetings without going to your Webex site.

Cisco Webex Productivity Tools is an optional companion application that allows users to quickly schedule and join meetings from their desktop without the need to access the Meetings website. The application should not be confused with the Cisco Webex Meetings Client, which is the main client application that provides the core functionality to host or attend a Webex meeting.

Administrators can update the Cisco Webex Meetings Desktop App or Webex Productivity Tools for their user base by following the instructions available in the document IT Administrator Guide for Mass Deployment of the Cisco Webex Meetings Desktop App and Productivity Tools.

Users can update the Cisco Webex Meetings Desktop App by launching the Cisco Webex Meetings application and clicking the gear icon in the top right of the application window and then choosing the **Check for Updates** entry from the drop-down list. This is also documented in the article Update the Cisco Webex Meetings Desktop App.

Users can update the Cisco Webex Productivity Tools in Microsoft Outlook by selecting **Schedule Meeting > More > Check for Updates**. This is also documented in more detail in the article Check for Cisco Webex Productivity Tools Updates for Windows.

Workarounds

There are no workarounds that address this vulnerability.

Fixed Software

When considering software upgrades, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories page, to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Fixed Releases

Customers are advised to upgrade to an appropriate fixed Cisco Webex Meetings Desktop App or Webex Productivity Tools software release as indicated in the following table:

Cisco Webex Platform	First Fixed Release
Webex Meetings Latest Channel sites	40.10
Webex Meetings Slow Channel sites	40.6
Webex Meetings Server	4.0MR3 SP4

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Source

This vulnerability was found during internal security testing.

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wda-pt-msh-6LWOcZ5

Revision History