Cisco Security Advisory

# Cisco Webex Meetings Enumeration Attack


**Advisory ID:** cisco-sa-20191001-webex-enum
**Published:** 2019 October 1 13:00 GMT
**Version1.0:** Final
**Workarounds:** Yes

Download PDF

Email

**Cisco Security Vulnerability Policy**

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

**Subscribe to Cisco Security Notifications**

Subscribe

**Summary**

Cisco Webex Meetings is an enterprise solution for hosting online meetings that offers video conferencing, screen sharing, and webinar capabilities that support hundreds of participants. Cisco Webex Meetings utilizes a nine-digit number as a user-friendly meeting identifier that can be easily typed in to join a meeting from all types of endpoints.

On July 24th, 2019, Shreyans Mehta of Cequence Security and the CQ Prime Research Team reported to Cisco that an attacker could take advantage of one of the Webex Meetings API calls to enumerate all the meeting numbers in use by an organization on the platform at a certain moment in time.

This advisory is available at the following link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191001-webex-enum

**Affected Products**

**Vulnerable Products**

The issue described in this advisory affects Cisco Webex Meetings.

**Products Confirmed Not Vulnerable**

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

Cisco has confirmed that Cisco Webex Meeting Server, used for on-premise deployments, does not exhibit this behavior.

**Details**

**As part of the process of creating a meeting, Webex will randomly generate and assign a nine-digit identifier that invitees can later use to join the meeting.**

**Shreyans Mehta of Cequence Security and the CQ Prime Research Team have reported to Cisco that one of the Webex API calls could be used to enumerate all of the meeting numbers for ongoing or future meetings. The response to the invoked API call would allow an attacker to determine:**

- **Whether a certain meeting number is in use, and**
- **Whether the meeting is password protected**

**The attacker could use the gathered information to try to join meetings that are not password protected. If the attacker was to join the meeting using this information, they would still be listed as a participant and could be expelled by the host. For password-protected meetings, the attacker could recover the meeting number, but would not be able to uncover the meeting title, schedule or host name, or join the meeting.**

**Workarounds**

**Fixed Software**

**Exploitation and Public Announcements**

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

**Source**

Cisco would like to thank Shreyans Mehta of Cequence Security and the CQ Prime Research Team for reporting this attack method.

**URL**

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191001-webex-enum

---

**Revision History**

| Version | Description | Section | Status | Date |
|---|---|---|---|---|
| 1.0 | Initial public release. | - | Final | 2019-October-01 |

---

**Legal Disclaimer**