



CVE-2020-3588

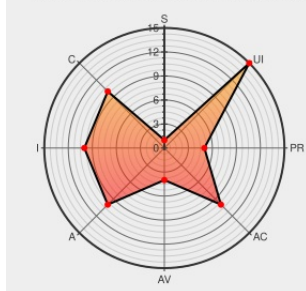
Published on: 11/06/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:39 PM UTC

CVE-2020-3588 - advisory for cisco-sa-webex-vdi-qQrpBwuJ

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Webex Meetings](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in virtualization channel messaging in Cisco Webex Meetings Desktop App for Windows could allow a local attacker to execute arbitrary code on a targeted system. This vulnerability occurs when this app is deployed in a virtual desktop environment and using virtual environment optimization. This vulnerability is due to improper

validation of messages processed by the Cisco Webex Meetings Desktop App. A local attacker with limited privileges could exploit this vulnerability by sending malicious messages to the affected software by using the virtualization channel interface. A successful exploit could allow the attacker to modify the underlying operating system configuration, which could allow the attacker to execute arbitrary code with the privileges of a targeted user. Note: This vulnerability can be exploited only when Cisco Webex Meetings Desktop App is in a virtual desktop environment on a hosted virtual desktop (HVD) and is configured to use the Cisco Webex Meetings virtual desktop plug-in for thin clients.

CVE-2020-3588 has been assigned by [Cisco PSIRT](#) to track the vulnerability - currently rated as **HIGH** severity.

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.

Affected Vendor/Software: [Cisco](#) - **Cisco Webex Meetings Desktop App** version **n/a**

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Cisco Webex Meetings Desktop App Arbitrary Code Execution Vulnerability	Patch Vendor Advisory tools.cisco.com text/html	CISCO 20201104 Cisco Webex Meetings Desktop App Arbitrary Code Execution Vulnerability
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Webex Meetings	All	All	All	All
Application	Cisco	Webex Meetings	All	All	All	All
cpe:2.3:a:cisco:webex_meetings:*:*:*:*:windows:*:*:						
cpe:2.3:a:cisco:webex_meetings:*:*:*:*:windows:*:*:						

No vendor comments have been submitted for this CVE