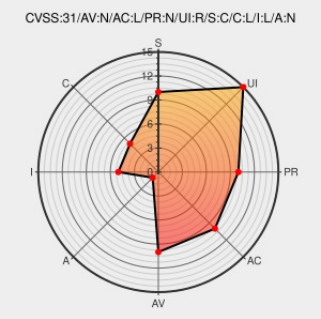
CVE-2020-27126

Published on: 11/18/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:27 PM UTC

CVE-2020-27126 - advisory for cisco-sa-webex-meetings-xss-MX56prER

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Webex Meetings from Cisco contain the following vulnerability:

A vulnerability in an API of Cisco Webex Meetings could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks. The vulnerability is due to improper validation of user-supplied input to an application programmatic interface (API) within Cisco Webex Meetings. An attacker could exploit this vulnerability by convincing a targeted user to follow a link designed to submit malicious input to the API used by Cisco Webex Meetings. A successful exploit could allow the attacker to conduct cross-site scripting attacks and potentially gain access to sensitive browser-based information from the system of a targeted user.

CVE-2020-27126 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM 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** version **n/a**

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality	**Integrity**	**Availability**

Impact	Impact	Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Cisco Webex Meetings API Cross-Site Scripting Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20201118 Cisco Webex Meetings API Cross-Site Scripting 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	40.10.2	All	All	All
Application	Cisco	Webex Meetings	40.10.2	All	All	All

cpe:2.3:a:cisco:webex_meetings:40.10.2:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:webex_meetings:40.10.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report