



CVE-2018-0390

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-0390
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-18 23:29:00 UTC
Updated	2019-10-09 23:31:00 UTC
Description	A vulnerability in the web framework of Cisco Webex could allow an unauthenticated, remote attacker to conduct a Document Object Model (DOM) based cross-site scripting (XSS) attack. An attacker could use this vulnerability to execute arbitrary scripts on an authenticated user's browser. An attacker could use this vulnerability to execute arbitrary scripts on an authenticated user's browser. An attacker could use this vulnerability to execute arbitrary scripts on an authenticated user's browser.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Webex Meetings	2.0	All	All	All
Application	Cisco	Webex Meetings	2.0	All	All	All

References

Reference	Source	Link	Tags
Cisco Webex DOM-Based Cross-Site Scripting Vulnerability	CONFIRM	tools.cisco.com	Vendor Advisory
Cisco WebEx CVE-2018-0390 Cross Site Scripting Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VDB Entry
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#).

Free CVE JSON API cve.report/api

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