



CVE-2017-3794

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

Summary

CVE	CVE-2017-3794
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-26 07:59:00 UTC
Updated	2017-07-26 01:29:00 UTC
Description	A vulnerability in Cisco WebEx Meetings Server could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against the Cisco WebEx Meetings Server. The vulnerability exists in the Cisco WebEx Meetings Server due to the lack of proper validation of the request parameters. An attacker could exploit this vulnerability to perform actions on behalf of the user without their knowledge or consent. The vulnerability is present in Cisco WebEx Meetings Server versions 2.6.0 through 2.6.1. Cisco has released a patch for this vulnerability in version 2.6.2.

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Webex Meetings Server	2.6.0	All	All	All
Application	Cisco	Webex Meetings Server	2.6.0	All	All	All

References

Reference	Source
Cisco WebEx Meetings Server Cross-Site Request Forgery Vulnerability	CO
Cisco WebEx Meetings Server CVE-2017-3794 Cross Site Request Forgery Vulnerability	BID
Cisco WebEx Meetings Server Access Control Flaw Lets Remote Users Conduct Cross-Site Request Forgery Attacks - SecurityTracker	SEI
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

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

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 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