



CVE-2014-3311

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

Summary

CVE	CVE-2014-3311
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-10 11:06:00 UTC
Updated	2017-08-29 01:34:00 UTC
Description	Heap-based buffer overflow in the file-sharing feature in WebEx Meetings Client in Cisco WebEx Meetings Server and Web

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Webex Meetings Server	-	All	All	All
Application	Cisco	Webex Meetings Server	-	All	All	All
Application	Cisco	Webex Meeting Center	-	All	All	All
Application	Cisco	Webex Meeting Center	-	All	All	All

References

Reference	Source
Cisco WebEx Meetings Server and WebEx Meeting Center Heap Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	SE
Cisco WebEx Meetings Client Heap-Based Buffer Overflow Vulnerability	CI
Cisco WebEx Meetings Client File Sharing Functionality Remote Heap Buffer Overflow Vulnerability	BI
IBM X-Force Exchange	XF
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.

© [CVE.report](#) 2026 |

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 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](#)