



CVE-2017-12311

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

Summary

CVE	CVE-2017-12311
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-16 07:29:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	A vulnerability in the H.264 decoder function of Cisco Meeting Server could allow an unauthenticated, remote attacker to ca

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Meeting Server	2.0	All	All	All
Application	Cisco	Meeting Server	2.1.0	All	All	All
Application	Cisco	Meeting Server	2.2.0	All	All	All
Application	Cisco	Meeting Server	2.3.0	All	All	All
Application	Cisco	Meeting Server	2.0	All	All	All
Application	Cisco	Meeting Server	2.1.0	All	All	All
Application	Cisco	Meeting Server	2.2.0	All	All	All
Application	Cisco	Meeting Server	2.3.0	All	All	All

References

Reference	Source
Cisco Meeting Server H.264 Decoding Denial of Service Vulnerability	CONFIRM
Cisco Meeting Server H.264 Processing Flaw Lets Remote Users Cause the Target Media Process to Restart - SecurityTracker	SECTRACK
Cisco Meeting Server H.264 Decoding CVE-2017-12311 Denial of Service Vulnerability	BID
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)