



CVE-2016-9218

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

Summary

CVE	CVE-2016-9218
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-26 07:59:00 UTC
Updated	2017-01-27 19:39:00 UTC
Description	A vulnerability in Cisco Hybrid Meeting Server could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against the Cisco Hybrid Meeting Server. The vulnerability is due to the Cisco Hybrid Meeting Server not validating the 'Referer' header in the HTTP request received by the Cisco Hybrid Meeting Server. An attacker could exploit this vulnerability to conduct a cross-site request forgery (CSRF) attack against the Cisco Hybrid Meeting Server. The attacker would need to be authenticated to the Cisco Hybrid Meeting Server in order to exploit this vulnerability. A successful exploit could allow the attacker to conduct a cross-site request forgery (CSRF) attack against the Cisco Hybrid Meeting Server.

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Hybrid Meeting Server	1.0_base	All	All	All
Application	Cisco	Hybrid Meeting Server	1.0_base	All	All	All

References

Reference	Source	Link	Tags
Cisco Hybrid Meeting Server Web Interface Cross-Site Request Forgery Vulnerability	CONFIRM	tools.cisco.com	Vendor Advisory
Cisco Hybrid Meeting Server CVE-2016-9218 Cross Site Request Forgery Vulnerability	BID	www.securityfocus.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, authoritative

No vendor comments have been submitted for this CVE.

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

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