



CVE-2016-6444

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2016-6444
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-27 21:59:15 UTC
Updated	2026-05-06 22:30:45 UTC
Description	A vulnerability in Cisco Meeting Server could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against the Cisco Meeting Server. The vulnerability is due to the Cisco Meeting Server not validating the 'Referer' header in the HTTP request received by the Cisco Meeting Server. An attacker could exploit this vulnerability to conduct a cross-site request forgery (CSRF) attack against the Cisco Meeting Server. Exploitation of this vulnerability requires that the attacker is on the same network as the Cisco Meeting Server. The vulnerability is present in Cisco Meeting Server versions 4.0.0 to 4.0.1. Cisco is releasing software updates to address this vulnerability. Customers are advised to upgrade to these updated versions as soon as possible. For more information on this vulnerability, please see the CVE entry for CVE-2016-6444.

Risk And Classification

Primary CVSS: v3.0 8.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

EPSS: 0.001940000 probability, percentile 0.410580000 (date 2026-05-09)

Problem Types: CWE-352 | unspecified

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Meeting Server	1.8.15	All	All	All
Application	Cisco	Meeting Server	1.8_base	All	All	All
Application	Cisco	Meeting Server	1.9.0	All	All	All
Application	Cisco	Meeting Server	1.9.2	All	All	All
Application	Cisco	Meeting Server	2.0.0	All	All	All
Application	Cisco	Meeting Server	2.0.1	All	All	All
Application	Cisco	Meeting Server	2.0.3	All	All	All
Application	Cisco	Meeting Server	2.0.4	All	All	All
Application	Cisco	Meeting Server	2.0.5	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Cisco Meeting Server 1.8 1.9 2.0	affected Cisco Meeting Server 1.8, 1.9, 2.0	Not specified

References

Reference	Source	Link
Cisco Meeting Server Cross-Site Request Forgery Vulnerability	af854a3a-2127-422b-91ae-364da2661108	tools.cisco.com

Cisco Meeting Server CVE-2016-6444 Cross Site Request Forgery Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com/bid/48800
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

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