



CVE-2015-0705

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2015-0705
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-22 01:59:00 UTC
Updated	2017-01-06 15:30:00 UTC
Description	Cross-site request forgery (CSRF) vulnerability in the SOAP API endpoints of the web-services directory in Cisco Unified M

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Unified Meetingplace	8.6(1.9)	All	All	All
Application	Cisco	Unified Meetingplace	8.6(1.9)	All	All	All
Application	Cisco	Unified Meetingplace	8.6(1.9)	All	All	All

References

Reference	Source
HPE Support document - HPE Support Center	CONF
20150421 Cisco Unified MeetingPlace Web Services Directory SOAP API Endpoints Cross-Site Request Forgery Vulnerability	CISCC
Cisco Unified MeetingPlace CVE-2015-0705 Cross Site Request Forgery Vulnerability	BID
Cisco Unified MeetingPlace SOAP API Endpoints Let Remote Users Conduct Cross-Site Request Forgery Attacks - SecurityTracker	SECTF
CVE Program record	CVE.C
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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)