



# CVE-2015-0704

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

## Summary

<b>CVE</b>	CVE-2015-0704
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-04-22 01:59:00 UTC
<b>Updated</b>	2017-01-06 16:29:00 UTC
<b>Description</b>	Multiple cross-site request forgery (CSRF) vulnerabilities in API features in Cisco Unified MeetingPlace 8.6(1.9) allow remote users to impersonate other users and perform actions on their behalf.

## 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
Cisco Unified MeetingPlace Server API Lets Remote Users Conduct Cross-Site Request Forgery Attacks - SecurityTracker	SECTRAK
Cisco Unified MeetingPlace Server Multiple State Changing URL API Functionalities Cross-Site Request Forgery Vulnerability	CISCO
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.

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](#)**