



CVE-2018-0359

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2018-0359 |
| State | PUBLIC |
| Assigner | psirt@cisco.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-06-21 11:29:00 UTC |
| Updated | 2019-10-09 23:31:00 UTC |
| Description | A vulnerability in the session identification management functionality of the web-based management interface for Cisco Meraki Meeting Server (MMS) allows an attacker to hijack the session of a user who is logged in to the MMS web interface. This vulnerability is caused by a session fixation attack. An attacker can hijack the session of a user who is logged in to the MMS web interface by sending a request to the MMS web interface with a session ID that is the same as the session ID of the user who is logged in to the MMS web interface. The attacker can then impersonate the user and perform actions on behalf of the user. |

Risk And Classification

Problem Types: CWE-384

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|----------------|---------|--------|---------|----------|
| Application | Cisco | Meeting Server | 2.3.0 | All | All | All |
| Application | Cisco | Meeting Server | 2.3.0 | All | All | All |

References

| Reference | Source | Link |
|--|----------|---|
| Cisco Meeting Server Session ID Re-use Lets Local Users Hijack the Target User's Session - SecurityTracker | SECTRACK | www.securitytracker.com/id/1041112 |
| Cisco Meeting Server Session Fixation Vulnerability | CONFIRM | tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-Security-Advisory-2018-0359 |
| Cisco Meeting Server CVE-2018-0359 Session Fixation Vulnerability | BID | www.securityfocus.com/bid/104111 |
| 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.

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](#)