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 Mee

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.securityt
Cisco Meeting Server Session Fixation Vulnerability	CONFIRM	tools.cisco.cor
Cisco Meeting Server CVE-2018-0359 Session Fixation Vulnerability	BID	www.securityf
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.

Free CVE JSON API cve.report/api

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