CVE-2017-12225

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-12225
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-07 21:29:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	A vulnerability in the web functionality of the Cisco Prime LAN Management Solution could allow an authenticated, remote a

Risk And Classification

Problem Types: CWE-384

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Prime Lan Management Solution	4.2(5)	All	All	All
Application	Cisco	Prime Lan Management Solution	4.2\(5\)	All	All	All
Application	Cisco	Prime Lan Management Solution	4.2\(5\)	All	All	All

References

Reference
Cisco Bug: CSCvf58392 - Cisco Prime LAN Management Solution Session Fixation Vulnerability
Cisco Prime LAN Management Solution Token ID Reuse Lets Remote Authenticated Users Hijack the Target User's Session - SecurityTracke
Cisco Prime LAN Management Solution Session Fixation Vulnerability
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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