



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 user to hijack the session of another user.

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 - SecurityTracker
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.

© [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](#)