CVE-2020-15259

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-15259
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-06 20:15:00 UTC
Updated	2020-11-18 21:16:00 UTC
Description	ad-ldap-connector's admin panel before version 5.0.13 does not provide csrf protection, which when exploited may result in

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Auth0	Ad/ldap Connector	All	All	All	All
Application	Auth0	Ad/ldap Connector	All	All	All	All

References

Reference	Source	Link	Tag
ad-ldap-connector admin console vulnerable to CSRF attack · Advisory · auth0/ad-ldap-connector · GitHub	CONFIRM	github.com	Thir
Merge pull request from GHSA-vx5q-cp9v-427v · auth0/ad-ldap-connector@8b79363 · GitHub	MISC	github.com	Patc
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

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

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