



CVE-2022-29773

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

Summary

CVE	CVE-2022-29773
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-03 21:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	An access control issue in aleksis/core/util/auth_helpers.py: ClientProtectedResourceMixin of AleksIS-Core v2.8.1 and below

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Aleksis	Aleksis	All	All	All	All

References

Reference	Source
AleksIS—Security Advisory: CVE-2022-29773 – Client-protected OAuth resources unprotected	MISC
ClientProtectedResourceMixin allows access if no allowed_scopes are set (#688) · Issues · AleksIS / Official / AleksIS-Core · GitLab	MISC
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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