CVE-2020-7674

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-7674
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-10 16:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	access-policy through 3.1.0 is vulnerable to Arbitrary Code Execution. User input provided to the `template` function is exec

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Access-policy Project	Access-policy	All	All	All	All

References

Reference	Source	Link	Tags
Arbitrary Code Execution in access-policy | Snyk	MISC	snyk.io	Exploit, Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981880 Nodejs (npm) Security Update for access-policy (GHSA-fw2f-7f87-5r6c)

Free CVE JSON API cve.report/api

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