



CVE-2023-40027

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-40027
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-15 18:15:00 UTC
Updated	2023-08-23 00:04:00 UTC
Description	Keystone is an open source headless CMS for Node.js — built with GraphQL and React. When `ui.isAccessAllowed` is set

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Keystonejs	Keystone	All	All	All	All

References

Reference	Score
Fix `ui.isAccessAllowed` when `undefined` to prevent access (#8771) · keystonejs/keystone@650e27e · GitHub	Medium
Fix `ui.isAccessAllowed` when `undefined` to prevent access by dcousens · Pull Request #8771 · keystonejs/keystone · GitHub	Medium
When `ui.isAccessAllowed` is undefined, the admin meta GraphQL query is publicly accessible · Advisory · keystonejs/keystone · GitHub	Medium
CVE Program record	Critical
NVD vulnerability detail	None

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[994862](#) NodeJs (Npm) Security Update for @keystone-6/core (GHSA-9cvc-v7wm-992c)

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)