



CVE-2022-39382

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

Summary

CVE	CVE-2022-39382
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-03 14:15:00 UTC
Updated	2022-11-04 16:08:00 UTC
Description	Keystone is a headless CMS for Node.js — built with GraphQL and React. `@keystone-6/core@3.0.0 3.0.1` users that use

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Keystonejs	Keystone	3.0.0	All	All	All
Application	Keystonejs	Keystone	3.0.1	All	All	All

References

Reference

- [Fixes platform configuration for esbuild by mmachatschek · Pull Request #8031 · keystonejs/keystone · GitHub](#)
- [NODE_ENV defaults to development with esbuild · Advisory · keystonejs/keystone · GitHub](#)
- [Test that process.env.NODE_ENV is production when set to that in production by mitchellhamilton · Pull Request #8063 · keystonejs/keystone](#)
- [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.

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](#)