



CVE-2022-36034

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

Summary

CVE	CVE-2022-36034
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-29 17:15:00 UTC
Updated	2023-07-21 20:52:00 UTC
Description	nitrado.js is a type safe wrapper for the Nitrado API. Possible ReDoS with lib input of `{` and with many repetitions of `{}`.

Risk And Classification

Problem Types: CWE-1333

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nitrado.js Project	Nitrado.js	All	All	All	All

References

Reference	Source	Link
Polynomial regular expression used on uncontrolled data in nitrado.js · Advisory · cainthebest/nitrado.js · GitHub	CONFIRM	github.com
nitrado.js/CHANGELOG.md at v0.2.5 · cainthebest/nitrado.js · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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