



CVE-2020-28925

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

Summary

CVE	CVE-2020-28925
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-30 19:15:00 UTC
Updated	2021-01-04 16:35:00 UTC
Description	Bolt before 3.7.2 does not restrict filter options in a Request in the Twig context, and is therefore inconsistent with the "How

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Boltcms	Bolt	All	All	All	All
Application	Boltcms	Bolt	All	All	All	All

References

Reference	Source	Link	Tags
Comparing 3.7.1...3.7.2 · bolt/bolt · GitHub	MISC	github.com	Patch, Third Party Advisory
Restrict `filter` options in `Request` in Twig context · bolt/bolt@c0cd530 · GitHub	MISC	github.com	Patch, 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

[905681](#) Common Base Linux Mariner (CBL-Mariner) Security Update for bolt (13769)

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