CVE-2020-4041

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

Summary

CVE	CVE-2020-4041
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-08 22:15:00 UTC
Updated	2022-10-07 01:24:00 UTC
Description	In Bolt CMS before version 3.7.1, the filename of uploaded files was vulnerable to stored XSS. It is not possible to inject jav

Risk And Classification

Problem Types: CWE-79

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
Check CSRF on Preview page by bobdenotter · Pull Request #7853 · bolt/bolt · GitHub	MISC	github.com	Patch, T
Full Disclosure: Bolt CMS <= 3.7.0 Multiple Vulnerabilities - CSRF to RCE	FULLDISC	seclists.org	
The filename of uploaded files vulnerable to stored XSS · Advisory · bolt/bolt · GitHub	CONFIRM	github.com	Patch, T
Merge pull request #7853 from bolt/fix/csrf-check-on-preview · bolt/bolt@b42cbfc · GitHub	MISC	github.com	Patch, T
Bolt CMS 3.7.0 XSS / CSRF / Shell Upload ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

905685 Common Base Linux Mariner (CBL-Mariner) Security Update for bolt (13765)

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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 registred 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