



CVE-2020-23960

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

Summary

CVE	CVE-2020-23960
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-11 16:15:00 UTC
Updated	2021-07-12 13:58:00 UTC
Description	Multiple cross-site request forgery (CSRF) vulnerabilities in the Admin Console in Fork before 5.8.3 allows remote attackers

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fork-cms	Fork	All	All	All	All
Application	Fork-cms	Fork	All	All	All	All
Application	Fork-cms	Fork Cms	All	All	All	All

References

Reference	Source	Link	Tags
Fork 5.8.3 released - Blog - Fork CMS	MISC	www.fork-cms.com	Release Notes, Vendor
Add more csrf checks by carakas · Pull Request #3123 · forkcms/forkcms · GitHub	MISC	github.com	Patch, Third Party Ad
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.

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](#).

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