

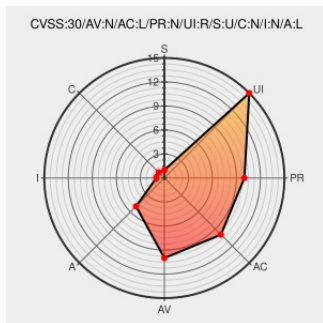


CVE-2022-3017

Published on: Not Yet Published

Last Modified on: 09/01/2022 07:38:00 PM UTC

CVE-2022-3017 - advisory for 5250c4b1-132b-4da6-9bd6-db36cb56bea0

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Froxlор](#) from [Froxlор](#) contain the following vulnerability:

Cross-Site Request Forgery (CSRF) in GitHub repository froxlор/froxlор prior to 0.10.38.

CVE-2022-3017 has been assigned by security@huntr.dev to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **froxlор** - **froxlор/froxlор** version < 0.10.38

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVE References

Description	Tags	Link
add security question for deleting api-keys to avoid accidental deletion · Froxlор/Froxlор@bbe8228 · GitHub	github.com text/html	MISC github.com/froxlор/froxlор/commit/bbe82286aee21328668f24857995a67598fe978a
huntr – Security Bounties for any GitHub repository	huntr.dev text/html Inactive Link Not Archived	CONFIRM huntr.dev/bounties/5250c4b1-132b-4da6-9bd6-db36cb56bea0

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Froxlор	Froxlор	All	All	All	All
cpe:2.3:a:froxlор:froxlор:*.***:*.***:.*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @vigilance_en	Vigil@nce #Vulnerability of Microsoft 365 Apps: code execution. vigilance.fr/vulnerability/... Identifiers: #CVE-2022-3017... twitter.com/i/web/status/1...	2022-06-15 07:09:04
 @threatmeter	CVE-2022-30176 Azure RTOS GUIX Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-3017... twitter.com/i/web/status/1...	2022-08-09 23:22:23
 @threatmeter	CVE-2022-30175 Azure RTOS GUIX Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-3017... twitter.com/i/web/status/1...	2022-08-09 23:22:23
 @threatmeter	CVE-2022-30176 Azure RTOS GUIX Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-3017... twitter.com/i/web/status/1...	2022-08-10 07:09:58
 @threatmeter	CVE-2022-30175 Azure RTOS GUIX Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-3017... twitter.com/i/web/status/1...	2022-08-10 07:09:59
 @huntrHacktivity	Cross-Site Request Forgery (CSRF) in github.com/froxlор/froxlор (CVE-2022-3017) reported by @vict0ni - Patch:... twitter.com/i/web/status/1...	2022-08-27 13:09:53
 @CVEreport	CVE-2022-3017 : Cross-Site Request Forgery CSRF in GitHub repository froxlор/froxlор prior to 0.10.38.... cve.report/CVE-2022-3017	2022-08-28 13:53:13
 @GeorgeKesaev	urgent CVE-2022-3017 Cross-Site Request Forgery (CSRF) in GitHub repository froxlор/froxlор prior to 0.10.38.	2022-08-28 14:51:53
 @Inceptus3	New Vulnerability: CVE-2022-3017 #InceptusSecure #UnderOurProtection	2022-08-28 16:12:17
 @0_exploit	CVE-2022-3017 dlvr.it/SXNLF8	2022-08-28 17:23:33
 /r/netcve	CVE-2022-3017	2022-08-28 14:38:10

[← Previous ID](#)
[Next ID →](#)

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](#)