



CVE-2022-29185

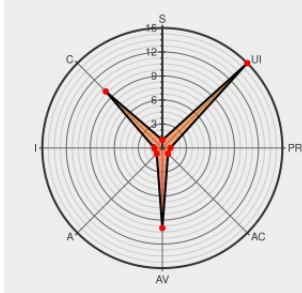
Published on: Not Yet Published

Last Modified on: 06/07/2022 09:19:00 PM UTC

CVE-2022-29185 - advisory for GHSA-8vxv-2g8p-2249

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

CVSS:31/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N



Certain versions of **Totp-rs** from **Totp-rs Project** contain the following vulnerability:

totp-rs is a Rust library that permits the creation of 2FA authentication tokens per time-based one-time password (TOTP). Prior to version 1.1.0, token comparison was not constant time, and could theoretically be used to guess value of an TOTP token, and thus reuse it in the same time window. The attacker would have to know the password beforehand nonetheless. Starting with patched version 1.1.0, the library uses constant-time comparison. There are currently no known workarounds.

CVE-2022-29185 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **constantoine** - **totp-rs** version <1.1.0

CVSS3 Score: **4.4 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link				
Release v1.1.0 · constantoine/totp-rs · GitHub	github.com text/html	MISC github.com/constantoine/totp-rs/releases/tag/v1.1.0				
Unsafe token check · Issue #13 · constantoine/totp-rs · GitHub	github.com text/html	MISC github.com/constantoine/totp-rs/issues/13				
Observable Timing Discrepancy in totp-rs · Advisory · constantoine/totp-rs · GitHub	github.com text/html	CONFIRM github.com/constantoine/totp-rs/security/advisories/GHSA-8vxv-2g8p-2249				
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 comment@cve.report.						
There are currently no QIDs associated with this CVE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Totp-rs Project	Totp-rs	All	All	All	All
cpe:2.3:a:totp-rs_project:totp-rs:*.***:*.rust:***:						
No vendor comments have been submitted for this CVE						
Social Mentions						
Source	Title					Posted (UTC)
@CVEreport	CVE-2022-29185 : totp-rs is a Rust library that permits the creation of 2FA authentication tokens per time-based... twitter.com/i/web/status/1...					2022-05-20 19:39:27
/r/netcve	CVE-2022-29185					2022-05-20 20:39:40
← Previous ID			Next ID →			