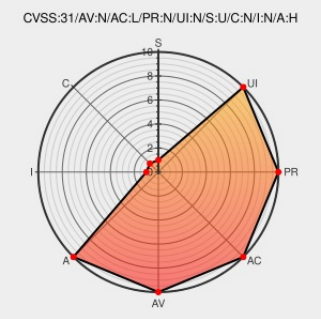
CVE-2023-33192

Published on: Not Yet Published

Last Modified on: 06/02/2023 06:10:00 PM UTC

CVE-2023-33192 - advisory for GHSA-qwhm-h7v3-mrjx

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ntpd-rs from Tweedegolf contain the following vulnerability:

ntpd-rs is an NTP implementation written in Rust. ntpd-rs does not validate the length of NTS cookies in received NTP packets to the server. An attacker can crash the server by sending a specially crafted NTP packet containing a cookie shorter than what the server expects. The server also crashes when it is not configured to handle NTS packets. The issue was caused by improper slice indexing. The indexing operations were replaced by safer alternatives that do not crash the ntpd-rs server process but instead properly handle the error condition. A patch was released in version 0.3.3.

CVE-2023-33192 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **pendulum-project** - **ntpd-rs** version **= >= 0.3.0, < 0.3.3**

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Cookie length validation by folkertdev · Pull Request #752 · pendulum-project/ntpd-rs · GitHub	github.com text/html	MISC github.com/pendulum-project/ntpd-rs/pull/752
Improper handling of NTS cookie length that could crash the ntpd-rs server · Advisory · pendulum-project/ntpd-rs · GitHub	github.com text/html	MISC github.com/pendulum-project/ntpd-rs/security/advisories/GHSA-qwhm-h7v3-mrjx

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	Tweedegolf	Ntpd-rs	All	All	All	All

cpe:2.3:a:tweedegolf:ntpd-rs:*:*:*:*:*:rust:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→