



CVE-2020-26235

Published on: 11/24/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:56 PM UTC

CVE-2020-26235 - advisory for GHSA-wcg3-cvx6-7396

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

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



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

In Rust time crate from version 0.2.7 and before version 0.2.23, unix-like operating systems may segfault due to dereferencing a dangling pointer in specific circumstances. This requires the user to set any environment variable in a different thread than the affected functions.

The affected functions are `time::UtcOffset::local_offset_at`,

`time::UtcOffset::try_local_offset_at`, `time::UtcOffset::current_local_offset`,

`time::UtcOffset::try_current_local_offset`, `time::OffsetDateTime::now_local` and

`time::OffsetDateTime::try_now_local`. Non-Unix targets are unaffected. This includes Windows and wasm. The issue was introduced in version 0.2.7 and fixed in version 0.2.23.

CVE-2020-26235 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [time-rs](#) - `time` version `>= 0.2.7, <0.2.23`

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

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

CVE References

Description	Tags	Link
crates.io: Rust Package Registry	Release Notes Vendor Advisory web.archive.org text/html Inactive Link Not Archived	 MISC crates.io/crates/time/0.2.23
The call to `localtime_r` may be unsound · Issue #293 · time-rs/time · GitHub	Issue Tracking Third Party Advisory github.com text/html	 MISC github.com/time-rs/time/issues/293
Potential segfault · Advisory · time-rs/time · GitHub	Patch Third Party Advisory github.com text/html	 CONFIRM github.com/time-rs/time/security/advisories/GHSA-wcg3-cvx6-7396

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.

Related QID Numbers

502891 Alpine Linux Security Update for newsboat

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Time Project	Time	All	All	All	All
Application	Time Project	Time	All	All	All	All
cpe:2.3:o:microsoft:windows:-:*.*****.*.*.*						
cpe:2.3:o:microsoft:windows:-:*.*****.*.*.*						
cpe:2.3:a:time_project:time:*.*****.*.*.*						
cpe:2.3:a:time_project:time:*.*****.*.*.*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @ttys22	CVE-2020-26235 #602 github.com/chronotope/chr...	2021-10-29

		15:06:27
 @first_issues	affected by CVE-2020-26235 via transitive dependencies github.com/kimono-koans/h... #github #Rust #Shell #Roff	2022-11-11 20:09:59
 /r/rust	What should we do about CVE-2020-26235 (localtime_r may be unsound)?	2021-11-10 13:07:52
← Previous ID		Next ID →

© CVE.report 2023   |

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 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](#)