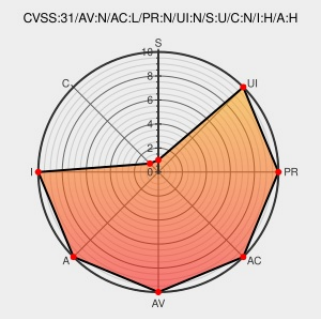
CVE-2020-35883

Published on: 12/31/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:48 PM UTC

CVE-2020-35883

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



Certain versions of Mozwire from Mozwire Project contain the following vulnerability:

An issue was discovered in the mozwire crate through 2020-08-18 for Rust. A ../ directory-traversal situation allows overwriting local files that have .conf at the end of the filename.

CVE-2020-35883 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.1 - CRITICAL

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

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
About RustSec › RustSec Advisory Database	Third Party Advisory rustsec.org text/html	MISC rustsec.org/advisories/RUSTSEC-2020-0030.html

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	Mozwire Project	Mozwire	All	All	All	All

cpe:2.3:a:mozwire_project:mozwire:*:*:*:*:*:rust:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report