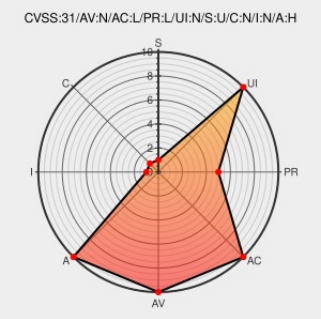
CVE-2022-31100

Published on: Not Yet Published

Last Modified on: 07/11/2022 02:00:00 PM UTC

CVE-2022-31100 - advisory for GHSA-8v9w-p43c-r885

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



Certain versions of Pomsky from Pomsky-lang contain the following vulnerability:

rulex is a new, portable, regular expression language. When parsing untrusted rulex expressions, rulex may crash, possibly enabling a Denial of Service attack. This happens when the expression contains a multi-byte UTF-8 code point in a string literal or after a backslash, because rulex tries to slice into the code point and panics as a result. This is a security concern for you, if your service parses untrusted rulex expressions (expressions provided by an untrusted user), and your service becomes unavailable when the thread running rulex panics. The crashes are fixed in version **0.4.3**. Affected users are advised to update to this version. The only known workaround for this issue is to assume that regular expression parsing will panic and to add logic to catch panics.

CVE-2022-31100 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **rulex-rs** - **rulex** version **< 0.4.3**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Fix panics due to slicing UTF8 strings incorrectly · rulex-rs/rulex@fac6d58 · GitHub	github.com text/html	MISC github.com/rulex-rs/rulex/commit/fac6d58b25c6f9f8c0a6cdc4dec75b37b219f1d6
Reachable Assertion in rulex · Advisory · rulex-rs/rulex · GitHub	github.com text/html	CONFIRM github.com/rulex-rs/rulex/security/advisories/GHSA-8v9w-p43c-r885

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pomsky-lang	Pomsky	All	All	All	All

cpe:2.3:a:pomsky-lang:pomsky:*:*:*:*:rust:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-31100 : rulex is a new, portable, regular expression language. When parsing untrusted rulex expressions, r… twitter.com/i/web/status/1…	2022-06-27 22:16:33
@threatmeter	CVE-2022-31100 rulex is a new, portable, regular expression language. When parsing untrusted rulex expressions, rul… twitter.com/i/web/status/1…	2022-06-28 07:09:42
/r/netcve	CVE-2022-31100	2022-06-27 23:38:33

← Previous ID

Next ID→

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