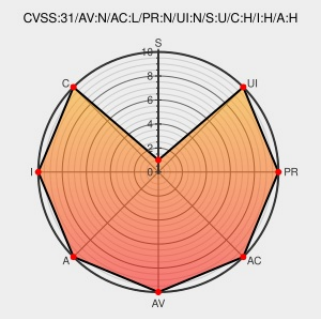
CVE-2023-23928

Published on: Not Yet Published

Last Modified on: 02/08/2023 01:27:00 AM UTC

CVE-2023-23928 - advisory for GHSA-7jj9-6qwv-wpm7

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



Certain versions of Reason-jose from Reason-jose Project contain the following vulnerability:

reason-jose is a JOSE implementation in ReasonML and OCaml.`Jose.Jws.validate` does not check HS256 signatures. This allows tampering of JWS header and payload data if the service does not perform additional checks. Such tampering could expose applications using reason-jose to authorization bypass. Applications relying on JWS claims assertion to enforce security boundaries may be vulnerable to privilege escalation. This issue has been patched in version 0.8.2.

CVE-2023-23928 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **ulrikstrid** - **reason-jose** version **= < 0.8.2**

CVSS3 Score: 9.8 - CRITICAL

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

CVE References

Description	Tags	Link
Merge pull request from GHSA-7jj9-6qwv-wpm7 · ulrikstrid/reason-jose@36cd724 · GitHub	github.com text/html	MISC github.com/ulrikstrid/reason-jose/commit/36cd724db3cbec121757624da49072386bd869e5
Jws ignores signature checks · Advisory · ulrikstrid/reason-jose · GitHub	github.com text/html	MISC github.com/ulrikstrid/reason-jose/security/advisories/GHSA-7jj9-6qwv-wpm7
Release 0.8.2 · ulrikstrid/reason-jose · GitHub	github.com text/html	MISC github.com/ulrikstrid/reason-jose/releases/tag/v0.8.2

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	Reason-jose Project	Reason-jose	All	All	All	All

cpe:2.3:a:reason-jose_project:reason-jose:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-23928 : reason-jose is a JOSE implementation in ReasonML and OCaml.`Jose.Jws.validate` does not check HS25… twitter.com/i/web/status/1…	2023-02-01 01:05:37
/r/netcve	CVE-2023-23928	2023-02-01 02:38:47

← Previous ID

Next ID→

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