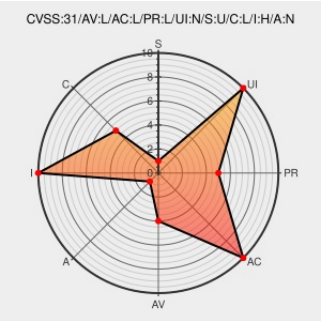
CVE-2022-36007

Published on: Not Yet Published

Last Modified on: 08/16/2022 05:02:00 PM UTC

CVE-2022-36007 - advisory for GHSA-4mmh-5vw7-rgvj

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



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

Venice is a Clojure inspired sandboxed Lisp dialect with excellent Java interoperability. A partial path traversal issue exists within the functions `load-file` and `load-resource`. These functions can be limited to load files from a list of load paths. Assuming Venice has been configured with the load paths: `[ "/Users/foo/resources" ]` When passing **relative** paths to these two vulnerable functions everything is fine: `(load-resource "test.png")` => loads the file "/Users/foo/resources/test.png" `(load-resource "../resources-alt/test.png")` => rejected, outside the load path When passing **absolute** paths to these two vulnerable functions Venice may return files outside the configured load paths: `(load-resource "/Users/foo/resources/test.png")` => loads the file "/Users/foo/resources/test.png" `(load-resource "/Users/foo/resources-alt/test.png")` => loads the file "/Users/foo/resources-alt/test.png" !!! The latter call suffers from the _Partial Path Traversal_ vulnerability. This issue's scope is limited to absolute paths whose name prefix matches a load path. E.g. for a load-path `"/Users/foo/resources"`, the actor can cause loading a resource also from `"/Users/foo/resources-alt"`, but not from `"/Users/foo/images"`. Versions of Venice before and including v1.10.17 are affected by this issue. Upgrade to Venice >= 1.10.18, if you are on a version < 1.10.18. There are currently no known workarounds.

CVE-2022-36007 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **jlangch** - **venice** version **<= 1.10.16**

CVSS3 Score: 3.3 - LOW

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

CVE References

Description	Tags	Link
Release Release 1.10.17 · jlangch/venice · GitHub	github.com text/html	MISC github.com/jlangch/venice/releases/tag/v1.10.17
vuln-fix: Partial Path Traversal Vulnerability · jlangch/venice@c942c73 · GitHub	github.com text/html	MISC github.com/jlangch/venice/commit/c942c73136333bc493050910f171a48e6f575
Merge pull request #4 from BulkSecurityGeneratorProjectV2/fix/JLL/par… · jlangch/venice@215ae91 · GitHub	github.com text/html	MISC github.com/jlangch/venice/commit/215ae91bb964013b0a2d70718a692832d56
Partial Path Traversal in com.github.jlangch:venice · Advisory · jlangch/venice · GitHub	github.com text/html	CONFIRM github.com/jlangch/venice/security/advisories/GHSA-4mmh-5vw7

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Venice Project	Venice	All	All	All	All

cpe:2.3:a:venice_project:venice:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-36007 : Venice is a Clojure inspired sandboxed Lisp dialect with excellent Java interoperability. A partia… twitter.com/i/web/status/1…	2022-08-14 00:29:34
/r/netcve	CVE-2022-36007	2022-08-14 01:38:27

← Previous ID

Next ID→