



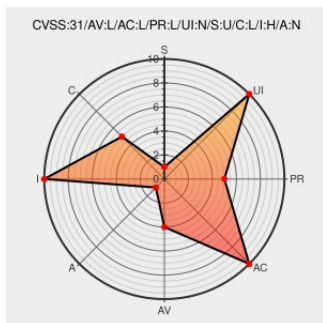
load-resource "/Users/foo/resources/test.png" ` ` => loads the file "/Users/foo/resources/test.png" ` ` (load-resource "../resources-alt/test.png") ` ` => loads the file "/Users/foo/resources/test.png" !!! The latter call suffers from the `_Partial Path Traversal_` vulnerability. This issue's scope is 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."> 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

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](mailto: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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <a href="#">github.com</a><br><a href="#">text/html</a> | MISC <a href="https://github.com/jlangch/venice/releases/tag/v1.10.17">github.com/jlangch/venice/releases/tag/v1.10.17</a>                                               |  |
| vuln-fix: Partial Path Traversal Vulnerability · jlangch/venice@c942c73 · GitHub                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <a href="#">github.com</a><br><a href="#">text/html</a> | MISC <a href="https://github.com/jlangch/venice/commit/c942c73136333bc493050910f171a48e6f575">github.com/jlangch/venice/commit/c942c73136333bc493050910f171a48e6f575</a> |  |
| Merge pull request #4 from BulkSecurityGeneratorProjectV2/fix/JLL/par... · jlangch/venice@215ae91 · GitHub                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <a href="#">github.com</a><br><a href="#">text/html</a> | MISC <a href="https://github.com/jlangch/venice/commit/215ae91bb964013b0a2d70718a692832d56">github.com/jlangch/venice/commit/215ae91bb964013b0a2d70718a692832d56</a>     |  |
| Partial Path Traversal in com.github.jlangch:venice · Advisory · jlangch/venice · GitHub                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <a href="#">github.com</a><br><a href="#">text/html</a> | CONFIRM <a href="https://github.com/jlangch/venice/security/advisories/GHSA-4mmh-5vw7">github.com/jlangch/venice/security/advisories/GHSA-4mmh-5vw7</a>                  |  |
| <p>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 <a href="mailto:comment@cve.report">comment@cve.report</a>.</p> |                                                         |                                                                                                                                                                          |  |

There are currently no QIDs associated with this CVE

| Known Affected Configurations (CPE V2.3)   |                                |                        |         |        |         |          |
|--------------------------------------------|--------------------------------|------------------------|---------|--------|---------|----------|
| Type                                       | Vendor                         | Product                | Version | Update | Edition | Language |
| Application                                | <a href="#">Venice Project</a> | <a href="#">Venice</a> | 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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-08-14 00:29:34 |
| /r/netcve       | <a href="#">CVE-2022-36007</a>                                                                                                                                                                           | 2022-08-14 01:38:27 |

© [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](#)