Partial Path Traversal in com.github.jlangch:venice

Moderate **jlangch** published **GHSA-4mmh-5vw7-rgvj** on Aug 12

Package

com.github.jlangch:venice (Maven)

Affected versions	Patched versions
<= 1.10.16	1.10.17

Description

Impact

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 v1.10.16 are affected by this issue.

Patches

Upgrade to Venice >= 1.10.17, if you are on a version < 1.10.17

Workarounds

If you cannot upgrade the library, you can control the functions that can be used in Venice with a sandbox. If it is appropriate, the functions `load-file` and `load-resource` can be blacklisted in the sandbox.

References

- PR

For more information

If you have any questions or comments about this advisory:

- Open an issue in GitHub Venice
- Email us at juerg.ch

Credits

I want to publicly recognize the contribution of Jonathan Leitschuh for reporting this issue.

Severity

Moderate

CVE ID

CVE-2022-36007

Weaknesses

CWE-22

Credits

JLLeitschuh