EEF-CVE-2026-32146

See a problem? Please try reporting it to the source first.

Source	https://cna.erlef.org/osv/EEF-CVE-2026-32146.html
Import Source	https://cna.erlef.org/osv/EEF-CVE-2026-32146.json
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2026-32146
Aliases	CVE-2026-32146 GHSA-vq5j-55vx-wq8j
Published	2026-04-11T12:59:22.911Z
Modified	2026-05-04T18:49:10.986Z
Severity	8.3 (High) CVSS_V4 - CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:N/VI:H/VA:N/SC:H/SI:H/SA:H CVSS Calculator
Summary	Improper Path Validation in Git Dependency Handling Allows Arbitrary File System Modification

Details

Summary

Improper path validation vulnerability in the Gleam compiler's handling of git dependencies allows arbitrary file system modification during dependency download.

Dependency names from gleam.toml and manifest.toml are incorporated into filesystem paths without sufficient validation or confinement to the intended dependency directory, allowing attacker-controlled paths (via relative traversal such as ../ or absolute paths) to target filesystem locations outside that directory. When resolving git dependencies (e.g. via gleam deps download), the computed path is used for filesystem operations including directory deletion and creation.

This vulnerability occurs during the dependency resolution and download phase, which is generally expected to be limited to fetching and preparing dependencies within a confined directory. A malicious direct or transitive git

dependency can exploit this issue to delete and overwrite arbitrary directories outside the intended dependency directory, including attacker-chosen absolute paths, potentially causing data loss. In some environments, this may be further leveraged to achieve code execution, for example by overwriting git hooks or shell configuration files.

This issue affects Gleam from 1.9.0-rc1 until 1.15.4.

Workaround

- Avoid using untrusted git dependencies, especially without pinning to a specific commit SHA
- Review dependency trees carefully, including transitive git dependencies
- Run dependency resolution commands in a restricted or isolated environment (e.g. containers)

Configuration

The project must use git-based dependencies (direct or transitive), or the victim must run gleam deps download on a repository with a malicious manifest.toml lockfile. Projects that exclusively use Hex dependencies and do not clone untrusted repositories are not affected.

Projects that exclusively use trusted or personally controlled git dependencies, or dependencies pinned to verified commit SHAs, are not exposed.

Database specific


```
{
    "capec_ids": [
        "CAPEC-139",
        "CAPEC-597"
    ],
    "cwe_ids": [
        "CWE-22"
    ],
    "cpe_ids": [
        "cpe:2.3:a:gleam-lang:gleam:*:*:*:*:*:*:*:*"
    ]
}
```


References

https://github.com/gleam-lang/gleam/security/advisories/GHSA-vq5j-55vx-wq8j

https://cna.erlef.org/cves/CVE-2026-32146.html

https://github.com/gleam-lang/gleam/commit/1aa5d8e594b0aa240bb213fce6ee19c65e6d5bcf

https://github.com/gleam-lang/gleam/commit/2dc0467f822c75de94697a912755d172928ee40a

Credits

John Downey - REMEDIATION_DEVELOPER

Louis Pilfold - ANALYST

Jonatan Männchen / EEF - COORDINATOR

Affected packages

Git
github.com/gleam-lang/gleam

Affected ranges

Type GIT

Repo https://github.com/gleam-lang/gleam

Events Introduced
a4fde22445ab8e5cc79c2ff48971616cb570702c
Fixed
92aae3913570e8d8962f6399404777d313045bfa
Fixed
2dc0467f822c75de94697a912755d172928ee40a

Affected versions

▸ v1.*

Database specific

▸ source