Improper Path Validation in Git Dependency Handling Allows Arbitrary File System Modification

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-32146
State	PUBLISHED
Assigner	EEF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-11 14:16:03 UTC
Updated	2026-04-11 14:16:03 UTC
Description	Improper path validation vulnerability in the Gleam compiler's handling of git dependencies allows arbitrary file system modi

Risk And Classification

Primary CVSS: v4.0 6.2 MEDIUM from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-22 | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	6.2	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:
4.0	CNA	CVSS	6.2	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Confidentiality

None

ntegrity

None

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Gleam	Gleam	affected 1.9.0-rc1 * semver	Not specified
CNA	Gleam	Gleam	affected 1.9.0-rc1 * semver	Not specified
CNA	Gleam	Gleam	affected a4fde22445ab8e5cc79c2ff48971616cb570702c * git	Not specified

References

Reference	Source	Link
github.com/gleam-lang/gleam/commit/1aa5d8e594b0aa240bb213fce6ee19c65e6d5bcf	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.c
osv.dev/vulnerability/EEF-CVE-2026-32146	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	osv.dev
cna.erlef.org/cves/CVE-2026-32146.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	cna.erle
github.com/gleam-lang/gleam/commit/55bb36e6d7febfbbc48c4d001e0ae13eb0312d78	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.c
github.com/gleam-lang/gleam/security/advisories/GHSA-vq5j-55vx-wq8j	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.c
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

Vendor Comments And Credit

Discovery Credit

CNA: John Downey (en)

CNA: Louis Pilfold (en)

CNA: Jonatan Männchen / EEF (en)

Additional Advisory Data

Workarounds

CNA: * 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)

There are currently no legacy QID mappings associated with this CVE.