Zip Slip Path Traversal

High **jdomeracki-coder** published **GHSA-8x9r-hvwg-c55h** 4 days ago

Package

code-marketplace (Go)

Affected versions	Patched versions
<= 2.4.1	2.4.2

Description

Zip Slip Path Traversal in coder/code-marketplace

Summary

A Zip Slip (CWE-22) vulnerability in `coder/code-marketplace` ≤ v2.4.1 allowed a malicious VSIX file to write arbitrary files outside the extension directory. `ExtractZip` passed raw zip entry names to a callback that wrote files via `filepath.Join` with no boundary check; `filepath.Join` resolved `..` components but did not prevent the result from escaping the base path.

Root Cause

`ExtractZip` passed the raw, attacker-controlled `zf.Name` to a caller-supplied callback:

```
return false, fn(zf.Name, zr)  // zf.Name not sanitized
```

`AddExtension` constructed the output path with `filepath.Join` and no boundary check:

```
path := filepath.Join(dir, name)              // zip loop
path := filepath.Join(dir, file.RelativePath) // extra files loop
```

`filepath.Clean` resolved `..` lexically but did not confine the result to `dir`:

```
filepath.Join("/srv/ext/pub/1.0", "../../../../etc/cron.d/evil")
  → "/etc/cron.d/evil"
```

Attack Scenario

An authenticated user (any upload-capable role) would submit a VSIX containing path-traversal entries.

On extraction, files would land at attacker-chosen paths writable by the marketplace process, enabling persistence (cron/init injection), SSH key injection, `ld.so.preload` hijacking, or binary overwrite depending on process privileges.

Fix

Addressed in https://github.com/coder/code-marketplace/releases/tag/v2.4.2

Recognition

We'd like to thank Kandlaguduru Vamsi for responsibly disclosing this issue in accordance with https://coder.com/security/policy

Severity

High

CVE ID

CVE-2026-35454

Weaknesses

▶ CWE-22

Credits

vamsik2k5 Finder