# CVE Detail – CVE-2022-24877

Flux is an open and extensible continuous delivery solution for Kubernetes. Path Traversal in the kustomize-controller via a malicious `kustomization.yaml` allows an attacker to expose sensitive data from the controller’s pod filesystem and possibly privilege escalation in multi-tenancy deployments. Workarounds include automated tooling in the user's CI/CD pipeline to validate `kustomization.yaml` files conform with specific policies. This vulnerability is fixed in kustomize-controller v0.24.0 and included in flux2 v0.29.0.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.68973

## CVSS Scoring

CVSS v3.1 Score: 9.9

Severity: CRITICAL

## Mapped CWE(s)

* CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
* CWE-36: Absolute Path Traversal

## CAPEC(s)

* CAPEC-126: Path Traversal
* CAPEC-597: Absolute Path Traversal
* CAPEC-64: Using Slashes and URL Encoding Combined to Bypass Validation Logic
* CAPEC-76: Manipulating Web Input to File System Calls
* CAPEC-78: Using Escaped Slashes in Alternate Encoding
* CAPEC-79: Using Slashes in Alternate Encoding

## Affected Products

* cpe:2.3:a:fluxcd:flux2:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:fluxcd:kustomize-controller:\*:\*:\*:\*:\*:\*:\*:\*