# CWE Detail – CWE-424

## Description

The product does not sufficiently protect all possible paths that a user can take to access restricted functionality or resources.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2022-29238: Access-control setting in web-based document collaboration tool is not properly implemented by the code, which prevents listing hidden directories but does not prevent direct requests to files in those directories.

## Related Attack Patterns (CAPEC)

* CAPEC-127
* CAPEC-554

## Attack TTPs

**•** T1083: File and Directory Discovery (Tactics: discovery)

## Modes of Introduction

**•** Architecture and Design: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism, Gain Privileges or Assume Identity — Notes:

## Potential Mitigations

**•** Architecture and Design: Deploy different layers of protection to implement security in depth. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)