# CVE Detail – CVE-2022-31503

The orchest/orchest repository before 2022.05.0 on GitHub allows absolute path traversal because the Flask send\_file function is used unsafely.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.66998

## CVSS Scoring

CVSS v3.1 Score: 9.3

Severity: CRITICAL

## Mapped CWE(s)

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

## CAPEC(s)

* CAPEC-126: 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:orchest:orchest:\*:\*:\*:\*:\*:\*:\*:\*