# CVE Detail – CVE-2024-37032

Ollama before 0.1.34 does not validate the format of the digest (sha256 with 64 hex digits) when getting the model path, and thus mishandles the TestGetBlobsPath test cases such as fewer than 64 hex digits, more than 64 hex digits, or an initial ../ substring.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.99838

## CVSS Scoring

CVSS v3.1 Score: 8.8

Severity: HIGH

## 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:ollama:ollama:\*:\*:\*:\*:\*:\*:\*:\*