# CVE Detail – CVE-2020-4053

In Helm greater than or equal to 3.0.0 and less than 3.2.4, a path traversal attack is possible when installing Helm plugins from a tar archive over HTTP. It is possible for a malicious plugin author to inject a relative path into a plugin archive, and copy a file outside of the intended directory. This has been fixed in 3.2.4.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.60343

## CVSS Scoring

CVSS v3.1 Score: 3.7

Severity: LOW

## 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:helm:helm:\*:\*:\*:\*:\*:\*:\*:\*