# CVE Detail – CVE-2019-20916

The pip package before 19.2 for Python allows Directory Traversal when a URL is given in an install command, because a Content-Disposition header can have ../ in a filename, as demonstrated by overwriting the /root/.ssh/authorized\_keys file. This occurs in \_download\_http\_url in \_internal/download.py.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.69143

## CVSS Scoring

CVSS v3.1 Score: 7.5

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:pypa:pip:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:leap:15.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:leap:15.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:9.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_cloud\_native\_core\_network\_function\_cloud\_native\_environment:1.10.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_cloud\_native\_core\_network\_function\_cloud\_native\_environment:22.1.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_cloud\_native\_core\_policy:1.15.0:\*:\*:\*:\*:\*:\*:\*