# CVE Detail – CVE-2022-20775

Multiple vulnerabilities in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges. These vulnerabilities are due to improper access controls on commands within the application CLI. An attacker could exploit these vulnerabilities by running a malicious command on the application CLI. A successful exploit could allow the attacker to execute arbitrary commands as the root user.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.3287

## CVSS Scoring

CVSS v3.1 Score: 7.8

Severity: HIGH

## Mapped CWE(s)

* CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
* CWE-25: Path Traversal: '/../filedir'

## 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:cisco:catalyst\_sd-wan\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:cisco:catalyst\_sd-wan\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:cisco:catalyst\_sd-wan\_manager:20.8:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:cisco:sd-wan\_vbond\_orchestrator:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:cisco:sd-wan\_vbond\_orchestrator:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:cisco:sd-wan\_vbond\_orchestrator:20.8:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:cisco:sd-wan\_vsmart\_controller:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:cisco:sd-wan\_vsmart\_controller:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:cisco:sd-wan\_vsmart\_controller:20.8:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:cisco:sd-wan:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:cisco:sd-wan:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:cisco:sd-wan:20.8:\*:\*:\*:\*:\*:\*:\*