



CVE-2020-3379

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2020-3379 |
| State | PUBLIC |
| Assigner | psirt@cisco.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-07-16 18:15:00 UTC |
| Updated | 2021-08-06 18:59:00 UTC |
| Description | A vulnerability in Cisco SD-WAN Solution Software could allow an authenticated, local attacker to elevate privileges to Adm |

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------|--------------------|---------|--------|---------|----------|
| Operating System | Cisco | Sd-wan Firmware | All | All | All | All |
| Operating System | Cisco | Sd-wan Firmware | All | All | All | All |
| Application | Cisco | Vbond Orchestrator | - | All | All | All |
| Application | Cisco | Vbond Orchestrator | - | All | All | All |
| Hardware | Cisco | Vedge 100 | - | All | All | All |
| Hardware | Cisco | Vedge 100 | - | All | All | All |
| Hardware | Cisco | Vedge 1000 | - | All | All | All |
| Hardware | Cisco | Vedge 1000 | - | All | All | All |
| Hardware | Cisco | Vedge 100b | - | All | All | All |
| Hardware | Cisco | Vedge 100b | - | All | All | All |
| Hardware | Cisco | Vedge 100m | - | All | All | All |
| Hardware | Cisco | Vedge 100m | - | All | All | All |
| Hardware | Cisco | Vedge 100wm | - | All | All | All |
| Hardware | Cisco | Vedge 100wm | - | All | All | All |
| Hardware | Cisco | Vedge 2000 | - | All | All | All |
| Hardware | Cisco | Vedge 2000 | - | All | All | All |
| Hardware | Cisco | Vedge 5000 | - | All | All | All |

| | | | | | | |
|-------------|-------|-------------------|---|-----|-----|-----|
| Hardware | Cisco | Vedge 5000 | - | All | All | All |
| Application | Cisco | Vsmart Controller | - | All | All | All |
| Application | Cisco | Vsmart Controller | - | All | All | All |

References

| Reference | Source | Link | Tags |
|---|---------|---|---------------------|
| Cisco SD-WAN Solution Software Privilege Escalation Vulnerability | CISCO | tools.cisco.com | Vendor Advisory |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

CVE.report and Source URL Uptime Status status.cve.report