



# CVE-2018-0342

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-0342
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-07-18 23:29:00 UTC
<b>Updated</b>	2019-10-09 23:31:00 UTC
<b>Description</b>	A vulnerability in the configuration and monitoring service of the Cisco SD-WAN Solution could allow an authenticated, local

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Cisco</a>	<a href="#">Vbond Orchestrator</a>	-	All	All	All
Application	<a href="#">Cisco</a>	<a href="#">Vbond Orchestrator</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">Vedge-100</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">Vedge-100</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">Vedge-1000</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">Vedge-1000</a>	-	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Vedge-1000 Firmware</a>	All	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Vedge-1000 Firmware</a>	All	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Vedge-100 Firmware</a>	All	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Vedge-100 Firmware</a>	All	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">Vedge-2000</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">Vedge-2000</a>	-	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Vedge-2000 Firmware</a>	All	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Vedge-2000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">Vedge-5000</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">Vedge-5000</a>	-	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Vedge-5000 Firmware</a>	All	All	All	All

Operating System	Cisco	Vedge-5000 Firmware	All	All	All	All
Application	Cisco	Vedge-plus	-	All	All	All
Application	Cisco	Vedge-plus	-	All	All	All
Application	Cisco	Vedge-pro	-	All	All	All
Application	Cisco	Vedge-pro	-	All	All	All
Hardware	Cisco	Vedge 100b	-	All	All	All
Hardware	Cisco	Vedge 100b	-	All	All	All
Operating System	Cisco	Vedge 100b Firmware	All	All	All	All
Operating System	Cisco	Vedge 100b Firmware	All	All	All	All
Hardware	Cisco	Vedge 100m	-	All	All	All
Hardware	Cisco	Vedge 100m	-	All	All	All
Operating System	Cisco	Vedge 100m Firmware	All	All	All	All
Operating System	Cisco	Vedge 100m Firmware	All	All	All	All
Hardware	Cisco	Vedge 100wm	-	All	All	All
Hardware	Cisco	Vedge 100wm	-	All	All	All
Operating System	Cisco	Vedge 100wm Firmware	All	All	All	All
Operating System	Cisco	Vedge 100wm Firmware	All	All	All	All
Application	Cisco	Vmanage Network Management	-	All	All	All
Application	Cisco	Vmanage Network Management	-	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 Local Buffer Overflow Vulnerability	CONFIRM	<a href="https://tools.cisco.com">tools.cisco.com</a>	Vendor Advisory
Cisco SD-WAN Solution CVE-2018-0342 Local Buffer Overflow Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory, VI
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**