

Date: December 23, 2025

| Revision | Date | Changes |
|----------|-------------------|--------------------------|
| 1.0 | October 16, 2019 | Initial release |
| 1.1 | December 23, 2025 | Updated to Arista Format |

NOTICE: VeloCloud is now an [Arista product](#).

Arista Networks has reposted this advisory that was originally posted by VMware October 16, 2019

The CVE-ID tracking this issue: [CVE-2019-5533](#)

CVSSv3.1 Base Score: 4.3

This vulnerability was originally published as VMSA-2019-0017

Description

Arista SD-WAN by VeloCloud update addresses information disclosure vulnerability.

The VeloCloud Orchestrator parameter authorization check mistakenly allows enterprise users to obtain information of Managed Service Provider accounts.

Impact: An enterprise user who is authenticated to the VeloCloud Orchestrator is able to retrieve information of users that are of type "MSP". Among this information is username, first and last name, phone numbers and e-mail address if present but no other personal data.

This issue was responsibly disclosed by Silas Bärtsch of Compass Security. Arista is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

VMware SD-WAN by VeloCloud (VeloCloud)

Versions

- 3.x

Affected Platforms

The following products **are** affected by this vulnerability:

- VMware SD-WAN by VeloCloud (VeloCloud)

The following product versions and platforms **are not** affected by this vulnerability:

- Arista EOS-based products:
 - 710 Series
 - 720D Series
 - 720XP/722XPM Series
 - 750X Series
 - 7010 Series
 - 7010X Series
 - 7020R Series
 - 7130 Series running EOS
 - 7150 Series
 - 7160 Series
 - 7170 Series
 - 7050X/X2/X3/X4 Series
 - 7060X/X2/X4/X5/X6 Series
 - 7250X Series
 - 7260X/X3 Series
 - 7280E/R/R2/R3 Series
 - 7300X/X3 Series
 - 7320X Series
 - 7358X4 Series
 - 7368X4 Series
 - 7388X5 Series
 - 7500E/R/R2/R3 Series
 - 7800R3/R4 Series
 - 7700R4 Series
 - AWE 5000 Series
 - AWE 7200R Series
 - CloudEOS
 - cEOS-lab
 - vEOS-lab
 - CloudVision eXchange, virtual or physical appliance
- Arista Wireless Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- CloudVision AGNI
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- Arista DANZ Monitoring Fabric (formerly Big Switch BMF)
- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
- Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)

- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)

Mitigation

No mitigations exist

Resolution

The recommended resolution is to upgrade to a remediated software version at your earliest convenience. Arista recommends customers move to the latest version of each release that contains all the fixes listed below.

CVE-2019-5533 has been fixed in the following releases:

- 3.3.1

VMware-hosted VeloCloud Orchestrators have been patched for this issue.

Hotfix

No Hotfix's are available for this issue

For More Information

If you require further assistance, or if you have any further questions regarding this security notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

Open a Service Request

Contact information needed to open a new service request may be found at:

<https://www.arista.com/en/support/customer-support>