Date: December 23, 2025

Revision	Date	Changes
1.0	July 5, 2020	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 July 5, 2020

The CVE-ID tracking this issue: CVE-2020-3973
CVSSv3.1 Base Score: 8.5
This vulnerability was originally published as VMSA-2020-0016

Description

An SQL-injection vulnerability in VeloCloud was privately reported to VMware. Patches are available to remediate this vulnerability in affected VMware products. VMware-hosted VeloCloud Orchestrators have been patched for this issue.

The VeloCloud Orchestrator does not apply correct input validation which allows for blind SQL-injection. VMware has evaluated the severity of this issue to be in the important severity range with a maximum CVSSv3 base score of 8.5.

A malicious actor with tenant access to Velocloud Orchestrator could enter specially crafted SQL queries and obtain data to which they are not privileged.

VMware would like to thank the UK's National Cyber Security Centre (NCSC) and Olivier Houssenbay from ON-X Securité for independently reporting this issue to us.

Vulnerability Assessment

Affected Software

VeloCloud Orchestrator

Versions

- 3.x

Affected Platforms

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

- VeloCloud Orchestrator

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:

- 3.3.2 p2
- 3.4.1 and above
- or apply a patch to 3.2.2, 3.3.1, 3.3.2 or 3.4.0

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