

CVE-2026-114625

Arista VeloCloud Orchestrator SQL Injection Vulnerability

Exigent

CISA KEV since Oct 23, 2026

Actively exploited

VeloCloud Orchestrator (VCO) on-prem has a security issue where this issue may allow a remote attacker to access privileged internal functionality and impact the VCO host. Successful exploitation may compromise the confidentiality, integrity, and availability of the orchestrator and data managed by the orchestrator. On an affected system, any authenticated user can gain operator privileges and masquerade as a local "superuser operator" user.

EVRS 85/100 Immediate priority	CVSS V4.0 9.4 Critical · NVD	EPSS 0.006 45.6th percentile · FIRST	CISA DEADLINE Oct 26, 2026 CISA federal deadline in 3 days
--	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☒ KEV recency	Added to CISA KEV within the last 30 days
☒ EPSS	0.006 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.4	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

This includes access to functionality that is intended for internal use only and which is not intended to be remotely accessible. Hosted, including Dedicated, versions of VCO were impacted and have already been patched.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
velocloud orchestrator	$\geq 5.2.0 < 5.2.3.18$ $\geq 6.1.0 < 6.1.3.10$ $\geq 6.4.0 < 6.4.2.12$	$5.2.3.18 \cdot 6.1.3.10 \cdot 6.4.2.12$	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-964w-6mm5-rm95	Additional guidance	arista.com/en/support/advisories-notices/security-advisory/24838-security-advisory-0199
BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk	Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk
NVD	nvd.nist.gov/vuln/detail/CVE-2026-114625	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-108511	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-114625

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.