An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2609230327

NCSC Advisory

Critical vulnerability in Arista Networks: VeloCloud Orchestrator (VCO) On-Prem

CVE-2026-93952

23rd, September 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-93952

Published: 2026-09-22

Vendor: Arista Networks

Product: VeloCloud Orchestrator (VCO) On-Prem

CVSS Score[1]: 10

Products Affected

Product	Version
VeloCloud Orchestrator (VCO) On-Prem	<= 5.2.3.15
VeloCloud Orchestrator (VCO) On-Prem	<= 6.1.3.7
VeloCloud Orchestrator (VCO) On-Prem	<= 6.4.2.7
VeloCloud Orchestrator (VCO) On-Prem	<= 7.0.0.2

Impact

VeloCloud Orchestrator (VCO) on-prem has a security issue. 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.

Hosted, including Dedicated, versions of VCO were impacted and have already been patched.

Common Weakness Enumeration (CWE)[2]: CWE-20 Improper Input Validation

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Arista Networks.

- https://nvd.nist.gov/vuln/detail/CVE-2026-93952
- https://www.cve.org/CVERecord?id=CVE-2026-93952
- https://www.arista.com/en/support/advisories-notices/security-advisory/24765-security-advisory-0183
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-93952