

Critical Input Validation Flaw in Arista VeloCloud Orchestrator Requires Immediate Patching



A critical improper input validation vulnerability in Arista VeloCloud Orchestrator on-premises deployments may allow remote attackers to access privileged functionality and compromise orchestrator confidentiality, integrity and availability.

- CVE-2026-93952 affects Arista VeloCloud Orchestrator on-premises installations with improper input validation
- Remote attackers may exploit the flaw to access privileged internal functionality and impact the host system
- Successful exploitation threatens confidentiality, integrity and availability of the orchestrator and managed data
- CISA directs organizations to apply vendor mitigations or discontinue product use if patches are

unavailable

- Asset owners must evaluate internet exposure and follow risk-based patching guidance

Vulnerability Overview

Arista VeloCloud Orchestrator on-premises deployments contain a critical **improper input validation vulnerability** tracked as CVE-2026-93952. The flaw may enable remote attackers to access privileged internal functionality and directly impact the orchestrator host system. Organizations using VeloCloud Orchestrator for SD-WAN management face potential compromise of confidentiality, integrity and availability across both the orchestrator platform and the data it manages.

Risk to Saudi Institutions

Regulated institutions in the Kingdom operating on-premises VeloCloud Orchestrator installations should treat this vulnerability as a priority remediation item. The vulnerability's remote exploitation vector and potential impact on privileged functionality represent significant risk to network management infrastructure. Financial institutions, healthcare providers and critical infrastructure operators relying on SD-WAN orchestration for branch connectivity or cloud access should assess their exposure immediately.

Remediation Guidance

CISA directs affected organizations to apply vendor-supplied mitigations in accordance with risk-based patching guidance. Where vendor patches or mitigations are not available, organizations should evaluate discontinuing use of the affected product. Asset owners must conduct an inventory of internet-exposed VeloCloud Orchestrator instances and prioritize remediation based on exposure level and criticality to operations. Organizations should document remediation activities and maintain forensic readiness in accordance with incident response procedures.

What to do now

1. Conduct an immediate inventory of all Arista VeloCloud Orchestrator on-premises installations across your organization
2. Identify internet-exposed VeloCloud Orchestrator instances and assess their criticality to business operations
3. Contact Arista Networks to obtain vendor-supplied patches or mitigations for CVE-2026-93952
4. Apply vendor mitigations following change management procedures and testing protocols
5. If patches are unavailable, evaluate risk tolerance and consider discontinuing use or isolating affected systems
6. Document all remediation activities and maintain forensic logs in accordance with NCA incident response

requirements