Arista warns of VeloCloud Orchestrator SQL injection zero-day under active exploitation



Arista says attackers are exploiting a zero-day SQL injection flaw in VeloCloud Orchestrator, the management system for VeloCloud SD-WAN. Any user who can log in, even read-only, can gain operator privileges.

- Arista published an advisory on October 22 confirming active exploitation.
- The flaw is a SQL injection zero-day in VeloCloud Orchestrator (VCO), the central management system for VeloCloud SD-WAN.
- Exploitation requires only a valid login, including a read-only customer account.
- Successful exploitation grants operator privileges, the highest level of control over the orchestrator.

What was reported

Arista stated in an advisory dated October 22 that attackers are already exploiting a zero-day SQL injection vulnerability in VeloCloud Orchestrator (VCO). VCO is the central management system for VeloCloud SD-WAN networks, so it holds control over how the wider network is configured and operated.

Why it matters

The flaw lowers the bar for attackers considerably. Anyone able to log in to the orchestrator can escalate to **operator** privileges, the top level of control, and this includes holders of a read-only customer account. An attacker therefore does not need an administrative foothold, only a valid set of credentials of any kind.

For institutions that use SD-WAN to connect branches, data centres and cloud services, a compromised orchestrator is a high-impact event. The source excerpt does not give further technical detail, affected versions or patch information, so those points should be confirmed directly from Arista's advisory.

Recommended approach

Treat this as an active-exploitation issue. Confirm whether your organisation, or a managed service provider acting for it, operates VeloCloud Orchestrator, and read the vendor advisory for mitigation steps. Review who holds accounts on the orchestrator, since even low-privilege accounts are relevant here, and check logs for unexpected privilege changes or new operator-level users.

What to do now

1. Identify whether VeloCloud Orchestrator is deployed in your environment or run for you by a service provider.
2. Read Arista's October 22 advisory and apply the mitigations or fixes it specifies.
3. Audit all accounts on the orchestrator, including read-only customer accounts, and remove those not needed.
4. Review orchestrator logs for unexpected privilege escalation or newly created operator-level users.
5. Restrict network access to the orchestrator management interface to trusted sources where possible.
6. Report confirmed compromise through your incident response process and notify NCA or SAMA as your obligations require.