Arista patches actively exploited VeloCloud Orchestrator zero-day (CVE-2026-114625)



Arista has patched CVE-2026-114625, a critical SQL injection flaw in on-prem VeloCloud Orchestrator that is being exploited in attacks. Any authenticated user can gain operator privileges. Administrators should patch and apply the interim steps.

- CVE-2026-114625 is a critical SQL injection flaw in VeloCloud Orchestrator (VCO) On-Prem and is exploited in the wild.
- An authenticated user with basic privileges can gain operator privileges and act as a local superuser operator.
- Arista has already patched hosted VCO deployments running 5.2.3.18 or later, 6.1.3.10 or later, and 6.4.2.12 or later.
- Arista lists two IP addresses seen in attacks: 74[.]82.197.86 and 38[.]54.50.151.

> - Arista has fixed three other exploited zero-days this year in EOS and on-prem VCO.

Arista Networks has released security updates for an actively exploited zero-day in VeloCloud Orchestrator (VCO) On-Prem, the web-based portal used to configure, monitor and manage VeloCloud SD-WANs and their edge devices.

What the flaw allows

The vulnerability, tracked as CVE-2026-114625, is rated critical. An attacker who has basic privileges, can reach the VCO web interface and holds a valid authenticated session can use a low-complexity SQL injection, with no user interaction, to escalate privileges. Arista says any authenticated user can obtain operator privileges and masquerade as a local superuser operator, reaching internal-only functionality. Exploitation may affect the confidentiality, integrity and availability of the orchestrator and the data it manages.

Arista has already patched hosted VCO deployments running 5.2.3.18 or later, 6.1.3.10 or later, and 6.4.2.12 or later. This is the fourth actively exploited zero-day Arista has addressed this year in EOS and on-prem VCO, after CVE-2026-7473, CVE-2026-16812 and CVE-2026-93952.

Interim measures from Arista

Until patches are applied, Arista advises restricting VCO web interface access to administrative networks, monitoring for connections from known malicious addresses, and reviewing recent administrator activity for unusual changes. It also suggests checking web access logs for unusual URL-like path components, encoded characters, references to local or internal services, and high request rates. The addresses 74[.]82.197.86 and 38[.]54.50.151 should be blocked.

If compromise is suspected, Arista recommends preserving web access, backend application, system and database logs and relevant file-system timestamps before remediation where operationally feasible, and contacting the Arista Technical Assistance Center (TAC).

What to do now

1. Identify all on-prem VCO instances and confirm the version against the fixed releases Arista lists; apply the update as soon as change control allows.
2. Restrict VCO web interface access to dedicated administrative networks until patching is complete.
3. Block 74[.]82.197.86 and 38[.]54.50.151 and search historical logs for connections from them.
4. Review VCO web access logs and recent administrator activity for encoded characters, internal-service references, high request rates and unexpected changes.
5. If compromise is suspected, preserve web, application, system and database logs and file-system timestamps before remediation, engage Arista TAC, and follow your incident response and regulator notification procedures.