VELOCLOUD / CVE-2026-114625

Read-only access. Operator privileges.

An actively exploited SQL injection flaw lets a valid VeloCloud Orchestrator login cross the operator boundary.

VALID PORTAL SESSION

Enterprise Read Only

↓

SQL INJECTION / REPORTED OUTCOME

Operator privileges

Enterprise Read Only is sufficient.

THE ACCESS PATH

A login is required. The role can be low.

Reach the web interface, hold a valid portal session, then exploit the affected Orchestrator.

01 / AUTHENTICATE

A valid portal session

↓

02 / EXPLOIT THE FLAW

Operator access

Edge and Gateway are not affected by this CVE.

PATCH CHECK

The September fix is not this fix.

If you still run the older builds below, check the new cutoff. Verify the running version, not just the ticket.

OLDER FIX		NEW CUTOFF
5.2.3.16	→	5.2.3.18
6.4.2.8	→	6.4.2.12

6.1 train: fixed in 6.1.3.10.
Later builds must be in the applicable train.

Use the fixed build in your release train.

INVESTIGATION LEADS

Check the addresses. Then check actions.

Arista published two attack source IPs. Search access records and correlate accounts, requests, and changes.

VENDOR-PUBLISHED SOURCE IPS

74.82.197.86

38.54.50.151

Review the activity behind the match.
Also check changes and outbound traffic.

A match is a lead, not proof of compromise.

MANAGEMENT AUTHORITY

What could that operator change?

Review the policies managed by your Orchestrator and the independent controls around them.

Who can reach the console?

Who approves policy changes?

Who retains the evidence?

For operational sites, the network design sets the risk.

CLOSEOUT

Fixed is one record. Investigated is another.

Keep the running-build check and the investigation result together, with named owners and open questions.

FIXED

Running build + exposure controls

INVESTIGATED

Reviewed activity + remaining gaps

Preserve evidence before remediation where feasible.