

Login Required | Active Exploitation | Operator Privileges | Fixed Releases Available

Executive Summary

The Cal-CSIC has become aware of a SQL injection vulnerability, CVE-2026-114625, affecting on-premises Arista VeloCloud Orchestrator. Arista rates the Critical vulnerability, with CVSS 3.1 and CVSS 4.0 base scores of 9.9 and 9.4, respectively. An attacker requires network access to the web interface and a valid portal session; the Enterprise Read Only role is sufficient. Successful exploitation allows the attacker to gain operator privileges and impersonate a local superuser operator, accessing privileged internal functionality and potentially compromising the host and managed data.[1] Arista has since released fixed versions and the vulnerability was confirmed to be actively exploited by the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities[2] catalog on October 23, 2026. Official sources do not provide runnable public proof-of-concept (PoC) code.

Recommended Actions

The Cal-CSIC recommends following the Arista Security Advisory[3] to include:

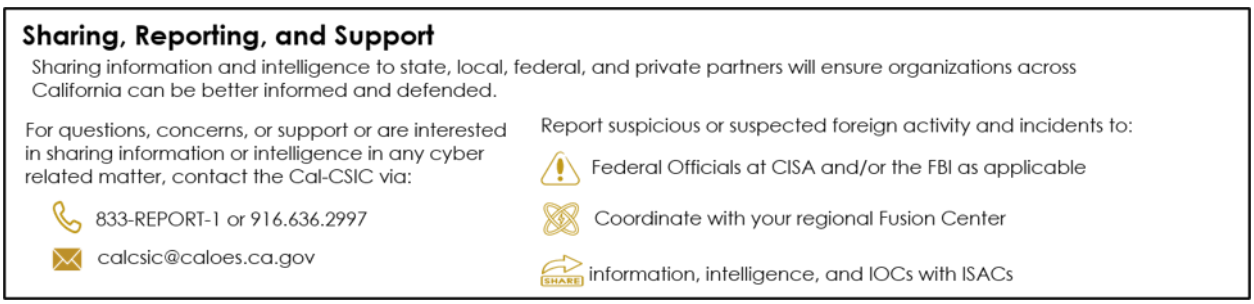
1. Installing the appropriate fixed release and prioritizing internet-facing systems.
2. Restrict portal access to trusted administrative networks pending the upgrade.
3. Investigate unexpected web requests, administrator changes, outbound connections and webshells.

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Affected Releases and Updated Version

Product	Affected range within branch	Updated version
Arista VeloCloud Orchestrator 5.2	5.2.0 to before 5.2.3.18	5.2.3.18 or later in 5.2
Arista VeloCloud Orchestrator 6.1	6.1.0 to before 6.1.3.10	6.1.3.10 or later in 6.1
Arista VeloCloud Orchestrator 6.4	6.4.0 to before 6.4.2.12	6.4.2.12 or later in 6.4

Sharing, Reporting, and Support



WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

References:

[1] NIST; "CVE-2026-114625 Detail"; https://nvd.nist.gov/vuln/detail/cve-2026-114625; Accessed 26 October 2026
[2] CISA; "Known Exploited Vulnerabilities catalog"; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-114625; Accessed 26 October 2026
[3] Arista Networks; "Security Advisory 0199"; https://www.arista.com/en/support/advisories-notices/security-advisory/24838-security-advisory-0199; Accessed 26 October 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.