EXPLOITED VULNERABILITY ADVISORY: CVE-2026-16812

Summary

CVE-2026-16812 affects Arista VeloCloud Orchestrator. It is being actively exploited in the wild (listed in the CISA Known Exploited Vulnerabilities catalogue). Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines. CISA remediation due 2026-07-30.

What we know

- **CVE:** CVE-2026-16812
- **Affected:** Arista VeloCloud Orchestrator
- **Exploitation:** Actively exploited, added to CISA KEV on 2026-07-27
- **Risk:** High
- **Weakness:** CWE-78

Required action

Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines. CISA remediation due 2026-07-30.

Source: CISA Known Exploited Vulnerabilities catalogue (public domain). An advisory of active exploitation, not an incident report; verify applicability to your estate before acting.