CYBERSECURITY RISK ADVISORY

Arista VeloCloud Orchestrator: Actively Exploited SQL Injection Zero-Day (CVE-2026-114625)

Network and infrastructure teams · Organizations running VeloCloud SD-WAN with an on-premises VeloCloud Orchestrator, and those relying on managed SD-WAN providers

ADVISORY ID	PUBLISHED	CLASSIFICATION	SEVERITY
SCA-ADV-2026-002	October 23, 2026 · v1.4 (updated November 19)	TLP:CLEAR	Critical

STATUS

Actively exploited · in CISA KEV

Developing situation. This advisory reflects public information as of **November 19, 2026, 12:00 PM Eastern Time**. **What changed in v1.4:** Arista's Advisory 0201 (first published October 23, revised to 1.5 on November 18) covers a separate problem: a compromised certificate authority key (eMudhra, CVE-2026-111943) that could expose VeloCloud Orchestrator, Edge and Gateway to man-in-the-middle attacks. Arista does not say it is being exploited. The orchestrator and Edge versions this advisory already recommends are newer than Arista's fixes for it; self-managed VeloCloud Gateways need 5.2.7.1, 6.1.6.1 or 6.4.4.1 or later.[13] CISA's catalog also marks CVE-2026-114625 as requiring a forensic triage, a check for prior compromise, under its directive BOD 26-04.[12] [14] Advisory 0199 is still at revision 1.0 and Advisory 0202 at revision 1.1.[1] [11] See our separate advisory SCA-ADV-2026-003 for HTTP2Shell. Each fact carries a numbered citation [1] that links to its source in Appendix A. The vendor's advisories are the primary sources; check them for revisions before acting. TLP:CLEAR means this advisory may be shared without restriction.[8]

1. Executive summary

On October 22, 2026, Arista disclosed **CVE-2026-114625**, a SQL injection flaw in the **VeloCloud Orchestrator (VCO)**, the central management system for VeloCloud SD-WAN.

Arista rates it **9.9 (Critical) under CVSS v3.1** and 9.4 under CVSS v4.0, and says it has detected **exploitation in the wild**.[1] An attacker who has any valid VCO login, even the lowest read-only role, can raise their privileges to operator level and act as a local superuser.[1] This is the third VeloCloud Orchestrator flaw reported as exploited since late July 2026, and the first that requires a login.[2]

Bottom line for executives

- **If you run an on-premises VeloCloud Orchestrator, treat it as urgent.** Upgrade to **5.2.3.20, 6.1.3.12 or 6.4.2.14** or later, which fix both this flaw and HTTP2Shell. The October fixes (5.2.3.18, 6.1.3.10, 6.4.2.12) close CVE-2026-114625 only. Arista has already patched its Hosted and Dedicated orchestrators for CVE-2026-114625.[1] [11] CISA gave federal agencies just three days, until October 26, to fix it.[9] [12]
- **Check your VeloCloud Edge devices too.** Arista added Edge to the HTTP2Shell advisory on November 12; fixed Edge releases are 7.0.1.1, 6.4.4.2, 6.1.6.2 and 5.2.7.2 or later, and there is no workaround.[11]
- **Earlier patches don't cover this.** Orchestrators upgraded for the July and September flaws are still exposed until they reach the new fixed versions.[2]
- **Patching alone may not be enough.** Arista advises hunting for backdoors and webshells, reviewing admin activity and preserving logs before you remediate. CISA requires federal agencies to carry out a forensic triage for this flaw, checking whether orchestrators were compromised before they were patched.[1] [12] [14]
- **Update self-managed VeloCloud Gateways.** A separate certificate-authority compromise (Arista Advisory 0201) affects them; fixed Gateway releases are 5.2.7.1, 6.1.6.1 and 6.4.4.1 or later. The orchestrator and Edge versions above already include Arista's fix.[13]

2. What happened

WHEN (2026)	EVENT	SOURCE
July	Arista patched CVE-2026-16812, a critical VeloCloud Orchestrator flaw that needs no login, after it was exploited in attacks. Canadian and New York State cyber agencies issued alerts.	[3] [4] [5]

WHEN (2026)	EVENT	SOURCE
September	A second exploited orchestrator flaw that needs no login, CVE-2026-93952, was disclosed. CISA added it to its Known Exploited Vulnerabilities (KEV) catalog on September 22.	[2] [6]
Oct 22	Arista published Security Advisory 0199 for CVE-2026-114625, reporting active exploitation and releasing fixes for the three affected orchestrator release trains (5.2, 6.1 and 6.4).	[1]
Oct 22–23	Security press reported the zero-day, which Arista found itself. Arista has not said when attacks began, which orchestrators were targeted or what attackers did afterward.	[2] [10]
Oct 23	CISA added CVE-2026-114625 to its Known Exploited Vulnerabilities catalog, giving federal agencies until October 26 to fix it.	[9]
Oct 27	CISA added HTTP2Shell (CVE-2026-111497), a flaw in Google's Brotli decoder, to its KEV catalog.	[12]
Nov 2	Arista published Security Advisory 0202: VeloCloud Orchestrator is affected by HTTP2Shell, with fixes in 5.2.3.20, 6.1.3.12 and 6.4.2.14. Arista rates it 9.8 under CVSS v3.1 for its products; the advisory does not report exploitation in them.	[11]
Nov 12	Arista revised Advisory 0202 to add VeloCloud Edge and DMF Analytics Node to the affected products.	[11]
Nov 17	Advisory 0199 for CVE-2026-114625 remains at revision 1.0, with no new indicators or versions.	[1]
Nov 18	Arista revised Advisory 0201 (revision 1.5, "Additional fixed versions published"). First published October 23, it covers the compromise of an eMudhra intermediate certificate authority key (CVE-2026-111943), which can expose software that trusts that authority to man-in-the-middle attacks. Affected: orchestrators up to 5.2.3.18, 6.1.3.10 and 6.4.2.12, and VeloCloud Edge and Gateway up to 5.2.7.0, 6.1.6.0, 6.2.0.1, 6.4.4.0 and 7.0.0.0. Arista reports no known reliable indicators of compromise.	[13]
Nov 19	Advisories 0199 (revision 1.0) and 0202 (revision 1.1) are unchanged. CISA's catalog lists CVE-2026-114625 as requiring forensic triage.	[1] [11] [12]

3. The vulnerability

The orchestrator does not properly sanitize some input, so a logged-in user can inject SQL commands into its database queries.[1]

CVE	WHAT GOES WRONG	SEVERITY	ACCESS NEEDED	IMPACT
CVE-2026-114625	SQL injection (CWE-89) in the VCO web interface[1]	CVSS v3.1 9.9 CVSS v4.0 9.4	Network access to the VCO web interface plus any valid account; minimum role Enterprise Read Only	Escalation to operator privileges; impersonation of a local superuser operator, including functions meant to be internal only

- **Why a login doesn't make this safe:** the lowest-privileged role, Enterprise Read Only, is enough.[1] In our experience, read-only, partner and monitoring accounts are often less protected than administrator accounts, so treat every login as a way in.
- **Exposure by default:** Arista says the VCO web interface is exposed by default and no VCO setting prevents that exposure.[1]
- **Not affected by CVE-2026-114625:** VeloCloud Gateway and Edge, Arista EOS products, CloudVision and Arista Wi-Fi.[1] VeloCloud Edge is, however, affected by the separate HTTP2Shell flaw.[11]
- **Second flaw on the same orchestrators:** HTTP2Shell (CVE-2026-111497) affects orchestrators up to 5.2.3.19, 6.1.3.11 and 6.4.2.13. Arista says it would need the orchestrator to fetch a crafted Brotli-compressed response through an outbound HTTP client, for example from an attacker-controlled or compromised integration endpoint, and that its review found no Brotli decoding in the inbound API request paths it checked. There is no workaround.[11]

4. Affected and fixed versions

ORCHESTRATOR RELEASE	VULNERABLE	FIXED IN	NOTES
6.4	Before 6.4.2.12	6.4.2.12	On-premises; 6.4.2.14 also fixes HTTP2Shell
6.1	Before 6.1.3.10	6.1.3.10	On-premises; 6.1.3.12 also fixes HTTP2Shell
5.2	Before 5.2.3.18	5.2.3.18	On-premises; 5.2.3.20 also fixes HTTP2Shell
Hosted and Dedicated	Were affected	Already patched by Arista	No customer action for this fix; still review admin activity

ORCHESTRATOR RELEASE	VULNERABLE	FIXED IN	NOTES
End-of-support releases	Not assessed	None listed	Contact Arista TAC

Version table from Arista's Advisory 0199; HTTP2Shell notes from Advisory 0202.[1] [11] Arista says releases not listed, including 7.0, are not vulnerable.[2] **If you patched in September:** the September fixes (5.2.3.16 and 6.4.2.8) predate this one, so those orchestrators still need the new versions.[2] **Recommended target now:** 5.2.3.20, 6.1.3.12 or 6.4.2.14 or later, per Arista Advisory 0202.[11]

Certificate authority compromise (Advisory 0201): Arista's fixes are orchestrator 5.2.3.19, 6.1.3.11 and 6.4.2.13 or later; Edge and Gateway 5.2.7.1, 6.1.6.1 and 6.4.4.1 or later. Arista's fix list names releases in the 5.2.7, 6.1.6 and 6.4.4 trains only; it lists Edge and Gateway 7.0.0.0 and earlier as affected without naming a 7.0 fix, so for other trains, including 6.2 and 7.0, ask Arista TAC. Until you can upgrade, Arista's interim step is to disable two root certificates (emSign ECC Root CA - G3 and AAA Certificate Services) in the host trust store and restart services, which it says reduces exposure but does not fully mitigate it. For Arista-hosted orchestrators, Arista says it verified that the server certificate chains in use do not include the affected intermediates.[13]

5. Exploitation and exposure

- **Confirmed exploitation:** Arista says it has detected exploitation of this flaw in the wild.[1]
- **Known attacker infrastructure:** Arista lists two IP addresses as indicators of compromise: `74.82.197[.]86` and `38.54.50[.]151`, which news reports geolocate to Japan.[1] [9] Arista has not attributed the activity to a threat actor.[9]
- **A pattern of attacks:** attackers have now exploited three different orchestrator flaws in about three months, which suggests sustained interest in this product.[2]
- **CISA's KEV catalog:** CISA added CVE-2026-114625 on October 23, 2026, with a federal due date of October 26.[9] CISA added the September flaw, CVE-2026-93952, in an alert dated September 22.[6] In the catalog version of November 18 (checked November 19), known ransomware campaign use for CVE-2026-114625 is listed as “Unknown,” and the entry is marked as requiring forensic triage under BOD 26-04.[12] [14]
- **HTTP2Shell:** CISA added CVE-2026-111497 to the KEV catalog on October 27. Arista's advisory does not report exploitation in its products; for Edge, Arista says its assessment

has not identified an actual exploit and no indicators of compromise are known.[11] [12]

9.9	3rd	2
CVSS v3.1 base score, scope changed[1]	exploited orchestrator flaw since late July 2026[2]	attacker IP addresses published by Arista[1]

6. Business risk

- **Control of your network management:** the orchestrator is the central management system for VeloCloud SD-WAN, and Arista says the flaw affects the confidentiality, integrity and availability of the orchestrator and the data it manages.[1] [10] In our assessment, superuser access could let an attacker change network configuration and site connectivity.
- **Reach into branch devices:** for the July and September flaws, Arista warned that a compromised orchestrator could give attackers access to VeloCloud Edge devices. It has not said whether that applies here, so plan as if it might.[2]
- **Persistence:** Arista's guidance to look for backdoor daemons and webshells means a patched orchestrator may still host an attacker who got in first.[1]
- **Managed-service exposure:** if a provider runs your SD-WAN, their on-premises orchestrator is your risk too. Ask for confirmation.
- **Reporting obligations:** if network or customer data was accessed, breach-notification laws, regulators, contracts and cyber insurance policies may set short deadlines. Involve counsel early.

7. Recommended actions

Today

1. **Find every orchestrator** you run, or that a provider runs for you, and record its version.
2. **Preserve evidence if compromise is possible:** Arista advises keeping web access, backend application, system and database logs and file-system timestamps before remediating, where feasible.[1]
3. **Upgrade** on-premises orchestrators to 5.2.3.20, 6.1.3.12 or 6.4.2.14 or later, which also fix HTTP2Shell. At minimum, reach 5.2.3.18, 6.1.3.10 or 6.4.2.12.[1] [11]
4. **Upgrade VeloCloud Edge** devices to 7.0.1.1, 6.4.4.2, 6.1.6.2 or 5.2.7.2 or later.[11]
5. **Upgrade self-managed VeloCloud Gateways** to 5.2.7.1, 6.1.6.1 or 6.4.4.1 or later for the certificate authority compromise; for other trains, including 6.2 and 7.0, ask Arista TAC.[13]
6. **If you can't upgrade today:** limit the VCO web interface to trusted administrative networks, and block or alert on the two published IP addresses.[1]
7. **Review accounts:** remove unused logins, including read-only, partner and service accounts, and reset credentials you can't vouch for.

Within 72 hours

1. **Run a forensic triage** on every orchestrator that was reachable before you patched, as CISA requires of federal agencies for this flaw: patching does not show whether an attacker got in first.[12] [14]
2. **Hunt for compromise:** look for backdoor daemons, webshells and unexpected changes made by administrators.[1]
3. **Watch outbound traffic** from the orchestrator host and consider blocking ports normal operation doesn't need, as Arista suggests.[1]
4. **Check edge and gateway configurations** for changes you didn't make.
5. **If you find signs of compromise,** treat it as an incident: contain, engage Arista TAC and incident response support, and check notification obligations.

Strategic

1. **Take management planes off the internet:** orchestrators, controllers and admin consoles belong behind a VPN or zero-trust access.
2. **Require multi-factor authentication** and least privilege for every management account, not only administrators.
3. **Move off end-of-support releases,** which Arista has not assessed.[1]
4. **Track CISA's KEV catalog** and set patch deadlines for exploited flaws in network infrastructure.[7]

8. What to watch for

- Connections to or from `74.82.197[.]86` or `38.54.50[.]151`.[1]
- In VCO web access logs: unusual URL-like path components, encoded characters, references to local or internal services, and high request rates.[1]
- Unexpected outbound network activity from the orchestrator host.[1]
- New daemons, unknown files in web directories, or administrator actions no one on your team performed.[1]

9. Questions for leadership

1. Do we run a VeloCloud Orchestrator ourselves, or through a provider, and which version is it on today?
2. Is its web interface reachable from the internet, and who decided that?
3. Did we patch the July and September flaws, and did we check for compromise then?
4. Are our orchestrators and Edge devices on the November fixed versions for HTTP2Shell, and our self-managed Gateways on Arista's fixed versions for Advisory 0201?
5. Has someone confirmed, through a forensic triage, that our orchestrators were not compromised before they were patched?

6. Who holds orchestrator logins, including read-only and partner accounts, and are they protected with multi-factor authentication?

Appendix A. Source map

Every citation, traced to its publisher. Sources were checked on October 23, 2026, new ones on October 25, 2026, and every citation was re-checked by an independent fact-checker on October 26, 2026. New sources for v1.3 were checked on November 17, 2026, and new ones for v1.4 on November 19, 2026, each round fact-checked independently. Arista's Advisory 0199 was still at revision 1.0, and Advisory 0202 at revision 1.1, on November 19.

#	WHAT IT SUPPORTS	SOURCE	TYPE	LINK
1	Security Advisory 0199 (Oct 22, 2026, revision 1.0): CVE-2026-114625; CWE-89; CVSS v3.1 9.9 and v4.0 9.4; exploitation detected; minimum role and privilege escalation; default exposure; affected and fixed versions; Hosted and Dedicated patched; end-of-support not assessed; products not affected; indicators of compromise; log preservation; mitigations	Arista Networks	Vendor	arista.com
2	Third exploited orchestrator flaw since late July and first requiring a login; CVE-2026-16812 (July) and CVE-2026-93952 (September); September fixed versions; earlier fixes still affected; 7.0 not vulnerable; Edge access warnings for earlier flaws; attack details not disclosed	The Hacker News, October 2026	Security news	thehackernews.com
3	Alert AV26-751 on Arista's July VeloCloud advisory	Canadian Centre for Cyber Security	Canadian government	cyber.gc.ca
4	Advisory 2026-072 on the July VeloCloud Orchestrator vulnerability	New York State Office of Information Technology Services	U.S. state government	its.ny.gov
5	July orchestrator zero-day exploited in attacks and patched	BleepingComputer	Security news	bleepingcomputer.com
6	CISA added CVE-2026-93952 to the KEV catalog (alert dated Sept 22, 2026; federal due date Sept 25)	Security Affairs, Sept 23, 2026	Security news	securityaffairs.com

#	WHAT IT SUPPORTS	SOURCE	TYPE	LINK
7	Known Exploited Vulnerabilities catalog (the page could not be loaded from our environment; the Oct 23 listing is reported by [9])	Cybersecurity and Infrastructure Security Agency (CISA)	U.S. government	cisa.gov
8	TLP:CLEAR definition; Traffic Light Protocol 2.0	FIRST	Standards body	first.org
9	CISA added CVE-2026-114625 to KEV (Oct 23, 2026), federal due date Oct 26; IOC IPs geolocated to Japan; no threat-actor attribution or victim count	The Hacker News, October 2026	Security news	thehackernews.com
10	Flaw found by Arista; impact on confidentiality, integrity and availability of the orchestrator and its managed data; third exploited orchestrator zero-day in four months; patches released Oct 22	SecurityWeek, Oct 23, 2026	Security news	securityweek.com
11	Security Advisory 0202 (Nov 2, 2026; revision 1.1, Nov 12): CVE-2026-111497 (HTTP2Shell); CVSS v3.1 9.8 and v4.0 9.2; affected and fixed VCO versions (5.2.3.20, 6.1.3.12, 6.4.2.14); Edge added in rev 1.1 with fixed versions; required configuration; no workaround; no exploitation reported; for Edge, no exploit identified and no known indicators of compromise	Arista Networks	Vendor	arista.com
12	KEV catalog version 2026.11.18, checked Nov 19 via CISA's official kev-data repository: CVE-2026-114625 (added Oct 23, due Oct 26, "forensicTriage: Yes") and CVE-2026-111497 (added Oct 27, due Nov 10); ransomware use "Unknown"	CISA Known Exploited Vulnerabilities catalog, via official kev-data repository	U.S. government	github.com/cisagov

#	WHAT IT SUPPORTS	SOURCE	TYPE	LINK
13	Security Advisory 0201 (first published Oct 23, 2026; revision 1.5, Nov 18, "Additional fixed versions published"), read Nov 19: eMudhra intermediate CA key compromise; CVE-2026-111943 (CWE-299, Arista-estimated CVSS v4.0 9.2); man-in-the-middle exposure; affected and fixed VCO, Edge and Gateway versions; no fixed 7.0 version named; interim trust-store steps; hosted VCO certificate chains verified; no exploitation reported and no reliable indicators of compromise	Arista Networks	Vendor (official)	arista.com
14	BOD 26-04, "Prioritizing Security Updates Based on Risk" (June 10, 2026), read Nov 19: "& forensic triage" means an agency must remediate within three days and "carry out a forensic triage of the asset to assess whether the system is compromised"; supersedes BOD 22-01 and BOD 19-02	Cybersecurity and Infrastructure Security Agency (CISA)	U.S. government	cisa.gov

Strat Cyber Advisors · Advisory SCA-ADV-2026-002 · v1.4 · Updated November 19, 2026 · **TLP:CLEAR**

This advisory summarizes public information for awareness and planning. It is not legal advice and does not replace guidance from your vendors or incident responders. Need help assessing exposure? Contact advisors@stratcyberadvisors.com.