Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Zero-Day Hits Arista VeloCloud Orchestrator

Date of Publication	Admiralty Code	TA Number
July 28, 2026	A1	TA2026212

Summary

First Seen: July 2026
Affected Products: Arista VeloCloud Orchestrator (VCO) On-Prem
Impact: Arista has patched a maximum-severity flaw in the on-premises version of its VeloCloud Orchestrator (VCO), the platform organizations used to centrally manage VeloCloud SD-WAN deployments and edge devices. Tracked as CVE-2026-16812, the bug is an unauthenticated OS command injection issue that lets a remote attacker reach privileged internal functionality never meant to be exposed to the outside world, without needing any tenant or operator credentials. Arista discovered the issue through external reporting and confirms it is already being actively exploited.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-16812	Arista VeloCloud Orchestrator On-Prem OS Command Injection Vulnerability	Arista VeloCloud Orchestrator (VCO)	✓	✓	✓

Vulnerability Details

#1

CVE-2026-16812 is an OS command injection vulnerability, classified under CWE-78 (Improper Neutralization of Special Elements used in an OS Command), affecting the on-premises deployment of Arista's VeloCloud Orchestrator. The flaw sits in internal functionality that was built for internal use only and was never intended to be reachable remotely, yet it is exposed to any network-level visitor of the VCO web interface by default.

#2

The root cause is that VCO fails to properly sanitize input before passing it through to underlying OS commands, allowing a remote and unauthenticated attacker to inject arbitrary operating system commands. No VCO tenant or operator credentials are required, and there is no user interaction needed, making this a straightforward point-and-shoot attack path for anyone with network access to the interface. Because the exposure cannot be disabled through configuration, the only mitigation short of patching is restricting network reachability to the interface itself.

#3

The vulnerability affects VCO on-prem releases in the 5.2.x branch prior to 5.2.3.14, the 6.1.x branch prior to 6.1.3.4, the 6.4.x branch prior to 6.4.2.4, and the 7.0.x branch before 7.0.0.1. VeloCloud Orchestrator Hosted and Dedicated deployments were already patched by Arista before the advisory was published and are not affected, and VeloCloud Gateway and VeloCloud Edge products are confirmed unaffected. End-of-support VCO release trains have not been assessed by Arista, so organizations still running them should treat their exposure as unknown and contact Arista's Technical Assistance Center for guidance. Organizations running any affected VCO on-prem release should patch to the latest available version on their respective train without delay to stay protected.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-16812	Arista VeloCloud Orchestrator (VCO) On-Prem (5.2.x before 5.2.3.14, 6.1.x before 6.1.3.4, 6.4.x before 6.4.2.4, 7.0.x before 7.0.0.1)	cpe:2.3:a:arista:velocloud_orchestrator:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Patch VCO Without Delay: Upgrade all on-premises VeloCloud Orchestrator instances to 5.2.3.14, 6.1.3.4, or 6.4.2.4 or later depending on your release train, or move to 7.0.0.1 or later. This is the only way to close the unauthenticated command injection path, and given confirmed active exploitation, it should be treated as an emergency change.

Restrict Web Interface Access: Until patching is complete, limit network reachability of the VCO web interface to trusted administrative networks only. Since the exposure cannot be turned off through VCO configuration itself, network-level controls such as firewall rules or access lists are the only interim defense.

Block Known Malicious IPs and Monitor Logs: Block the three IP addresses Arista has shared as observed attack sources: 8[.]19[.]75[.]217, 206[.]72[.]242[.]124, and 206[.]72[.]242[.]162, and review VCO web access logs, backend application logs, and system logs for connections from these addresses or other suspicious activity, since this list is not exhaustive.

Rotate Credentials and Validate Managed Devices: If compromise is suspected, preserve all relevant logs and file-system timestamps before remediation, then rotate credentials, review administrator activity, validate the state of managed devices, and consider restoring or replacing affected orchestrator instances from trusted sources, since a compromised VCO could also expose connected VeloCloud Edge devices.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	8[.]19[.]75[.]217, 206[.]72[.]242[.]124, 206[.]72[.]242[.]162

Patch Link

https://www.arista.com/en/support/advisories-notices/security-advisory/24364-security-advisory-0144

References

https://www.arista.com/en/support/advisories-notices/security-advisory/24364-security-advisory-0144

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

July 28, 2026 • 07:30 AM

More at www.hivepro.com