GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

28 July 2026

Advisory 175: Arista VeloCloud Orchestrator (VCO) On-Prem OS Command Injection Vulnerability (CVE-2026-16812)

Release Date: 27th July 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-16812 is a critical OS command injection vulnerability (CWE-78, CVSS v3.1 10.0) affecting the on-premises deployment of Arista VeloCloud Orchestrator (VCO) - the SD-WAN management/orchestration platform for VeloCloud Edge devices (formerly VeloCloud by Broadcom).

What are the systems affected?

The following on-premises product is affected:

- **VeloCloud Orchestrator (VCO) On-Prem (formerly VeloCloud Orchestrator by Broadcom)**

Affected software versions:

- VCO 5.2.x releases prior to 5.2.3.14
- VCO 6.1.x releases prior to 6.1.3.4
- VCO 6.4.x releases prior to 6.4.2.4
- VCO 7.0.x releases prior to 7.0.0.1

VeloCloud Orchestrator Hosted, VeloCloud Orchestrator Dedicated, VeloCloud Gateway, VeloCloud Edge, and Arista's EOS-based switching/routing products and CloudVision products are not affected by this vulnerability.

What does this mean?

Typical exploitation flow:

1. Target discovery
    - Attackers scan for internet-reachable VCO web interfaces; since VCO is exposed by default with no way to disable the exposure through configuration, any internet-facing VCO is a candidate.
2. Unauthenticated request to internal functionality
    - A crafted HTTP request reaches internal-only functionality that was never intended to be remotely reachable. No VCO credentials of any kind are required.
3. OS command injection
    - Improper neutralization of special elements in the request allows attacker-supplied input to be executed as an operating-system command on the VCO host.
4. Full host compromise
    - Successful exploitation may compromise the confidentiality, integrity, and availability of the orchestrator itself and of all data it manages.
5. Downstream impact on managed SD-WAN infrastructure
    - Because VCO manages VeloCloud Edge devices, a compromised orchestrator may in turn allow an attacker to reach or manipulate the Edge devices it manages.

This vulnerability requires:

- No authentication
- No user interaction
- Low attack complexity

Indicators of Compromise

Arista advises there is no single definitive indicator of compromise for this issue, but recommends reviewing VCO web access logs, backend application logs, and system logs for:

- Requests containing unusual URL-like path components, encoded characters, references to local/internal services, or unusually high request rates
- Unexpected outbound HTTP/HTTPS activity originating from the VCO host

- Sensitive configuration changes or privileged maintenance actions not tied to expected administrator activity
- Unexpected command execution, file creation, database export, or archive artefacts on the VCO host
- Unexpected access to VCO database contents, configuration data, device inventory, credentials, certificates, or key material

The following source IP addresses have been observed by Arista conducting attacks and should be blocked, with logs reviewed for any prior contact:

- 8.19.75.217
- 206.72.242.124
- 206.72.242.162

Mitigation process

CERTVU recommends the following:

1. **Apply Security Updates Immediately**
   - Upgrade on-premises VCO to a fixed release without delay: 5.2.3.14+ (5.2 train), 6.1.3.4+ (6.1 train), 6.4.2.4+ (6.4 train), or 7.0.0.1+ (7.0 train). This vulnerability is on the CISA Known Exploited Vulnerabilities (KEV) catalog and should be treated as an urgent remediation priority.
   - If your VCO is on an end-of-support release, contact Arista TAC to discuss upgrade options, as end-of-support versions have not been assessed for this issue.
2. **Restrict Network Exposure**
   - Restrict access to the VCO web interface to trusted administrative networks only, as an interim defense-in-depth control pending patching. Note this reduces but does not eliminate risk, since VCO is exposed by default.
3. **Monitor and Block Known Malicious Sources**
   - Block the three IP addresses listed above at the network/firewall level and review historical logs for any prior contact from them.

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-16812
3. https://www.arista.com/en/support/advisories-notices/security-advisory/24364-security-advisory-0144
4. https://cwe.mitre.org/data/definitions/78.html