Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0459

PRIORITEIT: NORMAAL

Kwetsbaarheid verholpen in Arista VeloCloud Orchestrator (VCO) on-premises

Publicatiedatum: 28-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (NCSC) verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Arista heeft een kritieke kwetsbaarheid verholpen in VeloCloud Orchestrator (VCO) On-Prem.

Duiding

De kwetsbaarheid met kenmerk CVE-2026-114625 heeft een CVSS-score van 9.9 en betreft SQL-injectie. Een geauthenticeerde kwaadwillende kan de kwetsbaarheid op afstand misbruiken om verhoogde rechten te verkrijgen en zich voor te doen als een lokale 'superuser operator'. Hierdoor kan de kwaadwillende toegang krijgen tot interne beheerfunctionaliteiten en mogelijk de vertrouwelijkheid, integriteit en beschikbaarheid van het systeem en de beheerde gegevens aantasten.

Voor succesvol misbruik heeft een kwaadwillende toegang nodig tot de webinterface van VCO en een geldige gebruikerssessie. Een account met de laagste standaardrechten, Enterprise Read Only, is hiervoor voldoende. Volgens Arista is de kwetsbare functionaliteit standaard blootgesteld en kan dit niet via een configuratiewijziging worden verholpen.

Succesvol misbruik kan leiden tot het verkrijgen van administratieve rechten en toegang tot interne functionaliteiten die normaal gesproken niet op afstand bereikbaar zijn. Hierdoor kunnen ook de door VCO beheerde netwerkomgevingen risico lopen.

De kwetsbaarheid maakt het mogelijk voor elke geauthenticeerde gebruiker met minimaal een Enterprise Read Only-rol om remote code uit te voeren en privileges te escaleren naar operatorniveau. Hierdoor krijgt de gebruiker toegang tot interne superuserfuncties. Het product is standaard blootgesteld zonder configuratieopties om deze aanvalsvector te beperken. Er zijn meldingen van kwaadaardige IP-adressen die exploitatiepogingen uitvoeren, waaronder 74.82.197.86 en 38.54.50.151. Hosted VCO-instanties hebben reeds patches ontvangen om dit probleem te verhelpen.

Arista bevestigt dat de kwetsbaarheid actief wordt misbruikt. Het NCSC adviseert om de beveiligingsupdates met spoed toe te passen en kwetsbare systemen te onderzoeken op aanwijzingen voor eerdere compromittering.

Oplossingen

Arista heeft beveiligingsupdates uitgebracht om de kwetsbaarheid te verhelpen. De kwetsbaarheid is verholpen in VCO 5.2.3.18, 6.1.3.10 en 6.4.2.12, of latere versies binnen de betreffende releasebranches. Hosted-omgevingen, waaronder Dedicated, zijn volgens Arista reeds bijgewerkt.

Totdat de beveiligingsupdates zijn geïnstalleerd, adviseert Arista de toegang tot de VCO-webinterface te beperken tot vertrouwde beheernetwerken.

Vanwege het actieve misbruik adviseert Arista daarnaast de webtoegangslogs te onderzoeken op verdachte verzoeken en activiteiten vanaf de IP-adressen 74.82.197[.]86 en 38.54.50[.]151. Bij vermoedelijke compromittering wordt door Arista geadviseerd relevante logbestanden en forensische gegevens veilig te stellen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.arista.com/en/support/advisories-notices/security-advisory/24838-security-advisory-0199

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-114625	9.4 CRITICAL

CWE's

CWE	Beschrijving
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Getroffen producten

Arista
VeloCloud Orchestrator

Arista Networks
VeloCloud Orchestrator

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:
NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.