



NCSC-2026-0385

Kwetsbaarheid verholpen in VeloCloud Orchestrator (VCO) on-premises

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 22-09-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het 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 delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

VeloCloud heeft een kwetsbaarheid verholpen in VeloCloud Orchestrator (VCO) on-premises.

Duiding

De kwetsbaarheid in VCO stelt externe aanvallers in staat om toegang te krijgen tot geprivilegieerde interne functionaliteit, wat de vertrouwelijkheid, integriteit en beschikbaarheid kan aantasten. De kwetsbaarheid wordt actief uitgebuit en is in hosted VCO-omgevingen reeds verholpen. Beperk de toegang tot de VCO-webinterface tot vertrouwde administratieve netwerken om de blootstelling aan de kwetsbaarheid te verminderen en monitor de omgeving op mogelijke compromittering.

Oplossingen

VeloCloud heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie het bijgevoegde beveiligingsadvies van Arista voor Indicators of Compromise (IoC's) en informatie over de beschikbare patches.

Dreigingsinformatie

Files

```
/usr/local/sbin/.vcnode.js
/usr/local/sbin/vc-sysmond
    Known malicious hash of file is (md5)
    "dc78e206eaeadec59fc5801fe4556bd0"
/etc/systemd/system/vc-sysmon.service
```

The following HTTP header in nginx logs

x-vc-opt

Connections from the following IP addresses

142.93.149.77
104.248.126.159

Kwetsbaarheden

CVE	CVSS Score
> CVE-2026-93952	9.5 CRITICAL

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Getroffen producten

Arista
VeloCloud Orchestrator On-Prem
Arista Networks
VeloCloud Orchestrator (VCO) On-Prem

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.