



NCSC-2025-0374

Kwetsbaarheden verholpen in Arista EOS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 20-11-2025

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

Arista heeft kwetsbaarheden verholpen in de Arista EOS-platform.

Duiding

De kwetsbaarheden zijn gerelateerd aan de verwerking van verkeerd gevormde berichten, wat kan leiden tot systeemcrashes en Denial-of-Service-omstandigheden. Aanvallers met hoge privileges kunnen deze kwetsbaarheden misbruiken, wat leidt tot ernstige operationele verstoringen. Daarnaast kan het verzenden van willekeurige bytes naar het CVX-systeem de ControllerOob-agent laten herstarten, wat ook kan resulteren in een Denial-of-Service. Bovendien heeft de Arista EOS-platform een kwetsbaarheid die systemen met IPsec beïnvloedt, waardoor de dataplane stopt met het verwerken van al het IPsec-verkeer. Dit kan een systeemreset vereisen, zonder garantie op herstel van de verkeersverwerking. Voor misbruik heeft de kwaadwillende geen authenticatie nodig. Tot slot kan een geauthenticeerde Redis-sessie volledige roottoegang krijgen tot alle servers binnen de CVX-cluster, wat een ernstige bedreiging vormt voor de beveiliging.

Oplossingen

Arista heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.arista.com/en/support/advisories-notices/security-advisory/22868-security-advisory-0126>
- <https://www.arista.com/en/support/advisories-notices/security-advisory/22869-security-advisory-0127>

Kwetsbaarheden

| CVE | CVSS Score |
|---------------------------------|------------|
| ➤ CVE-2025-5089 | 6.5 MEDIUM |
| ➤ CVE-2025-5090 | 6.5 MEDIUM |
| ➤ CVE-2025-8873 | 7.5 HIGH |
| ➤ CVE-2025-5088 | 8.3 HIGH |

CWE's

| CWE | Beschrijving |
|----------------------------|---|
| > CWE-20 | Improper Input Validation |
| > CWE-269 | Improper Privilege Management |
| > CWE-1286 | Improper Validation of Syntactic Correctness of Input |

Getroffen producten

| |
|------------------------|
| Arista Networks |
| EOS |

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.