Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0366

Kwetsbaarheden verholpen in Arista EOS

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-09-2026

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

Arista heeft kwetsbaarheden verholpen in de Arista EOS-platform.

Duiding

De kwetsbaarheid met kenmerk CVE-2026-73456 bevindt zich in de verwerking van verzoeken die via gNPSI worden aangeboden. Onder de kwetsbare configuratie kan een niet-geauthenticeerde client een kwaadaardig verzoek aanbieden waarmee code-injectie kan worden veroorzaakt. Een kwaadwillende met netwerktoegang tot de gNPSI-service kan zonder authenticatie een speciaal vervaardigd verzoek versturen waarmee willekeurige code kan worden uitgevoerd. Hierdoor kan de kwaadwillende volledige administratieve controle over de getroffen switch verkrijgen.

De kwetsbaarheid met kenmerk CVE-2026-73457, kan ertoe leiden dat gNPSI-clientgegevens, waaronder wachtwoorden, in plaintext in lokale of remote accounting logs terechtkomen. Een kwaadwillende met voldoende rechten om de betreffende logs te benaderen, kan deze gegevens vervolgens uitlezen. Volgens Arista is misrbuik mogelijk indien gNPSI is ingeschakeld én de trace facility EosRpcAuth expliciet is geactiveerd. gNPSI is standaard uitgeschakeld.

Volgens Arista is misbruik uitsluitend mogelijk wanneer gNPSI is ingeschakeld, in combinatie met specifieke TLS- en authenticatieconfiguraties, dan wel met een expliciet geactiveerde EosRpcAuth trace facility. Aangezien gNPSI standaard is uitgeschakeld, zijn systemen met de fabrieksinstellingen niet kwetsbaar.

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/24714-security-advisory-0158

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-73456	
CVE-2026-73457	

CWE's

CWE	Beschrijving
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-532	Insertion of Sensitive Information into Log File

Getroffen producten

Arista
EOS

Disclaimer