Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0294

Kwetsbaarheden verholpen in HPE Aruba Networking EdgeConnect SD-WAN Gateways

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 18-09-2025

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

HPE heeft kwetsbaarheden verholpen in HPE Aruba Networking EdgeConnect SD-WAN Gateways.

Duiding

De kwetsbaarheden bevinden zich in de command-line interface en web API van de HPE Aruba Networking EdgeConnect SD-WAN Gateways. Deze kwetsbaarheden stellen geauthenticeerde aanvallers in staat om willekeurige systeemcommando's uit te voeren met root-toegang, shell-toegang te verkrijgen, en processen te beëindigen, wat kan leiden tot ongeautoriseerde controle en destabilisatie van de systemen. Dit kan ook resulteren in het uitlekken van gevoelige gegevens en het omzeilen van bestaande firewallbescherming.

Oplossingen

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

Referenties

- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04943en_us&docLocale=en_US

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-37123	8.7 HIGH
CVE-2025-37124	6.9 MEDIUM
CVE-2025-37125	6.9 MEDIUM
CVE-2025-37126	8.6 HIGH
CVE-2025-37127	1.8 LOW
CVE-2025-37128	7.1 HIGH
CVE-2025-37129	8.4 HIGH
CVE-2025-37130	5.3 MEDIUM

CVE-2025-37131	**5.1 MEDIUM**

CWE's

CWE	Beschrijving
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-250	Execution with Unnecessary Privileges
CWE-269	Improper Privilege Management
CWE-284	Improper Access Control
CWE-287	Improper Authentication
CWE-310	CWE-310
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-404	Improper Resource Shutdown or Release
CWE-552	Files or Directories Accessible to External Parties
CWE-693	Protection Mechanism Failure

Getroffen producten

HPE
Aruba Networking EdgeConnect SD-WAN Gateway

Disclaimer