Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0016

Kwetsbaarheden verholpen in Aruba Networks ArubaOS

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 16-01-2026

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

Aruba Networks heeft kwetsbaarheden verholpen in AOS-8 en AOS-10.

Duiding

De kwetsbaarheden bevinden zich in de webmanagementinterfaces van de AOS-8 en AOS-10 systemen. Deze kwetsbaarheden omvatten onder andere een arbitrarily file deletion, stack overflow, command injection, en improper input handling. Een kwaadwillende kan deze kwetsbaarheden misbruiken om ongeautoriseerde toegang te verkrijgen, bestanden te verwijderen of te manipuleren, en zelfs commando's met verhoogde privileges uit te voeren.

Voor succesvol misbruik moet de kwaadwillende toegang hebben tot de management-interface, of de Command Line. Het is goed gebruik om een dergelijke interface niet publiek toegankelijk te hebben, maar af te steunen in een separate beheeromgeving.

Oplossingen

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

Referenties

- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04987en_us&docLocale=en_US

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-37168	8.2 HIGH
CVE-2025-37169	7.2 HIGH
CVE-2025-37170	7.2 HIGH
CVE-2025-37171	7.2 HIGH
CVE-2025-37172	7.2 HIGH
CVE-2025-37173	7.2 HIGH

CVE-2025-37174	7.2 HIGH
CVE-2025-37175	7.2 HIGH
CVE-2025-37176	6.5 MEDIUM
CVE-2025-37177	6.5 MEDIUM
CVE-2025-37178	5.3 MEDIUM
CVE-2025-37179	6.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-125	Out-of-bounds Read
CWE-277	Insecure Inherited Permissions
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-552	Files or Directories Accessible to External Parties

Getroffen producten

HPE
ArubaOS (AOS)

Disclaimer