Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# Advisory NCSC-2024-0220

## Kwetsbaarheden verholpen in Aruba Networks ArubaOS

2024-05-16 Revisie 0

### Toegestande verspreiding: 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.firs t.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

## Feiten

Aruba Networks heeft kwetsbaarheden verholpen in ArubaOS

## Interpretaties

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- Manipulatie van gegevens
- (Remote) code execution (Administrator/Root rechten)
- Toegang tot systeemgegevens

Voor succesvol misbruik moet de kwaadwillende toegang hebben tot de management interface (PAPI-poort). Het is goed gebruik deze interface niet publiek toegankelijk te hebben, maar af te steunen in een separaat beheer-LAN

## Oplossingen

Aruba Networks heeft updates uitgebracht om de kwetsbaarheden te verhelpen in ArubaOS 10.6.0.0, 10.5.1.1 en 10.4.1.1. Zie bijgevoegde referentie voor meer informatie:

## Referenties

- https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2024-006.txt