



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités affectant ArubaOS et Aruba SD-WAN
<b>Numéro de Référence</b>	28222212/20
<b>Date de Publication</b>	22 Décembre 2020
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- ArubaOS versions 6.4.4.x antérieures à 6.4.4.24
- ArubaOS versions 6.5.4.x antérieures à 6.5.4.18
- ArubaOS versions 8.2.2.x antérieures à 8.2.2.10
- ArubaOS versions 8.3.0.x antérieures à 8.3.0.14
- ArubaOS versions 8.5.0.x antérieures à 8.5.0.11
- ArubaOS versions 8.6.0.x antérieures à 8.6.0.6
- ArubaOS versions antérieures à 8.7.1.0
- Aruba SD-WAN versions 2.1.0.x antérieures à 2.1.0.2
- Aruba SD-WAN versions 2.2.0.x antérieures à 2.2.0.1

### Identificateurs externes

- CVE-2020-10713 CVE-2020-24633 CVE-2020-24634 CVE-2020-24637

### Bilan de la vulnérabilité

Aruba annonce la correction de plusieurs vulnérabilités qui affectent ses produits ArubaOS et Aruba SD-WAN. Un attaquant distant non authentifié pourrait exploiter ces failles afin d'injecter des commandes, d'exécuter du code arbitraire ou de contourner la politique de sécurité.

## Solution

Veillez-vous référer au bulletin de sécurité de ArubaNetworks afin d'installer les nouvelles mises à jour.

## Risque

- Injection de commandes à distance
- Exécution de code arbitraire à distance
- Contournement de la politique de sécurité

## Référence

Bulletin de sécurité d'ArubaNetworks:

- <https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-012.txt>