



## BULLETIN DE SECURITE

|                            |  |
|----------------------------|--|
| <b>Titre</b>               | Vulnérabilités critique dans Aruba ArubaOS |
| <b>Numéro de Référence</b> | 40570103 /23                               |
| <b>Date de Publication</b> | 02 Mars 2023                               |
| <b>Risque</b>              | Critique                                   |
| <b>Impact</b>              | Critique                                   |

### Systemes affectés

- ArubaOS versions 8.10.x.x antérieures à 8.10.0.5
- ArubaOS versions 8.11.x.x antérieures à 8.11.0.0
- ArubaOS versions 10.3.x.x antérieures à 10.3.1.1
- SD-WAN versions 8.7.0.0-2.3.0.x antérieures à 8.7.0.0-2.3.0.9

### Identificateurs externes

- CVE-2021-3712, CVE-2023-22747, CVE-2023-22748, CVE-2023-22749, CVE-2023-22750, CVE-2023-22751, CVE-2023-22752, CVE-2023-22753, CVE-2023-22754, CVE-2023-22755, CVE-2023-22756, CVE-2023-22757, CVE-2023-22758, CVE-2023-22759, CVE-2023-22760, CVE-2023-22761, CVE-2023-22762, CVE-2023-22763, CVE-2023-22764, CVE-2023-22765, CVE-2023-22766, CVE-2023-22767, CVE-2023-22768, CVE-2023-22769, CVE-2023-22770, CVE-2023-22771, CVE-2023-22772, CVE-2023-22773, CVE-2023-22774, CVE-2023-22775, CVE-2023-22776, CVE-2023-22777, CVE-2023-22778

### Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans Aruba ArubaOS. L'exploitation de ces failles pourrait permettre à un attaquant d'exécuter du code arbitraire à distance, de porter atteinte à la confidentialité des données et de contourner la politique de sécurité.

### Solution

Veuillez se référer au bulletin de sécurité Aruba du 28 février 2023 pour plus d'information.

### Risque

- Exécution du code arbitraire à distance
- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité

## Annexe

Bulletin de sécurité Aruba du 28 février 2023:

- <https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt>