



## BULLETIN DE SECURITE

|                            |  |
|----------------------------|--|
| <b>Titre</b>               | Vulnérabilités critiques affectant Aruba EdgeConnect Enterprise Orchestrator |
| <b>Numéro de Référence</b> | 38671310/22  |
| <b>Date de publication</b> | 13 Octobre 2022  |
| <b>Risque</b>              | Important  |
| <b>Impact</b>              | Critique   |

### Systemes affectés

- Aruba EdgeConnect Enterprise Orchestrator 9.2.0.40405 et versions antérieures
- Aruba EdgeConnect Enterprise Orchestrator 9.1.3.40197 et versions antérieures
- Aruba EdgeConnect Enterprise Orchestrator 9.0.7.40110 et versions antérieures
- Aruba EdgeConnect Enterprise Orchestrator 8.10.23.40015 et versions antérieures

### Identificateurs externes

- CVE-2022-37913 CVE-2022-37914 CVE-2022-37915

### Bilan de la vulnérabilité

Aruba Networks annonce la correction de trois vulnérabilités critiques affectant les versions susmentionnées de son produit Aruba EdgeConnect Enterprise Orchestrator. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire, de contourner l'authentification ou d'élever ses privilèges.

### Solution

Veillez se référer aux pages de mises à jour du constructeur pour mettre à jour vos équipements.

## Risques

- Exécution de code arbitraire
- Contournement de l'authentification
- Contrôle du système vulnérable

## Références

Bulletin de sécurité d'Aruba Networks

- <https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-015.txt>