



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités affectant plusieurs produits VMware
<b>Numéro de Référence</b>	39431212/22
<b>Date de publication</b>	12 Décembre 2022
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- ESXi versions 7.x antérieures à ESXi70U3si-20841705
- ESXi versions 6.7 antérieures à ESXi670-202210101-SG
- ESXi versions 6.5 antérieures à ESXi650-202210101-SG
- vCenter Server versions 7.x antérieures à 7.0 U3i
- vCenter Server versions 6.7 antérieures à 6.7.0 U3s
- vCenter Server versions 6.5 antérieures 6.5 U3u
- Cloud Foundation (ESXi) versions 4.x sans le correctif de sécurité KB90336
- Cloud Foundation (ESXi) versions 3.x sans le correctif de sécurité KB90336
- Cloud Foundation (vCenter Server) versions 4.x sans le correctif de sécurité KB90336
- Cloud Foundation (vCenter Server) versions 3.x sans le correctif de sécurité KB90336

### Identificateurs externes

CVE-2022-31696 CVE-2022-31697 CVE-2022-31698 CVE-2022-31699

### Bilan de la vulnérabilité

VMware annonce la correction de quatre vulnérabilités affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'accéder à des données confidentielles, de causer un déni de service ou de contourner les mesures de sécurité.

## Solution

Veillez se référer au bulletin de sécurité de VMware pour les mises à jour.

## Risques

- Déni de service
- Contournement des mesures de sécurité
- Accès à des données confidentielles

## Références

Bulletin de sécurité de VMware:

- <https://www.vmware.com/security/advisories/VMSA-2022-0030.html>