DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 20-10-2025

BULLETIN ALERTES

Object	Multiples vulnérabilités dans les produits VMware
Réference	1403
Date de Publication	2025-09-30
Sévérité	Elevé

IMPACT :

- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Élévation de privilèges

SYSTÉME AFFECTÉ :

- Aria Operations versions 8.x antérieures à 8.18.5
- Cloud Foundation versions 13.x antérieures à 13.0.5.0
- Cloud Foundation versions 4.5.x avec vCenter versions 7.x antérieures à 7.0 U3w
- Cloud Foundation versions 5.x antérieures à 5.2.2
- Cloud Foundation versions 5.x et 4.x sans les recommandations des articles KB92148 et KB88287
- Cloud Foundation versions 9.x antérieures à 9.0.1.0
- NSX versions 4.0.x et 4.1.x antérieures à 4.1.2.7
- NSX versions 4.2.2.x antérieures à 4.2.2.2
- NSX versions 4.2.3.x antérieures à 4.2.3.1
- NSX-T versions 3.x antérieures à 3.2.4.3
- Telco Cloud Infrastructure versions 3.x et 2.x avec Aria Operations versions 8.x antérieures à 8.18.5
- Telco Cloud Infrastructure versions 3.x et 2.x sans les recommandations des articles KB411508 et KB411518
- Telco Cloud Platform versions 5.x et 4.x avec Aria Operations versions 8.x antérieures à 8.18.5
- Telco Cloud Platform versions 5.x, 4.x, 3.x et 2.x sans les recommandations des articles KB411508 et KB411518
- vCenter versions 7.x antérieures à 7.0 U3w
- vCenter versions 8.x antérieures à 8.0 U3g
- VMware Tools versions 11.x et 12.x antérieures à 12.5.4
- VMware Tools versions 13.x antérieures à 13.0.5
- vSphere Foundation versions 13.x antérieures à 13.0.5.0
- vSphere Foundation versions 9.x antérieures à 9.0.1.0

DÉSCRIPTION :

Plusieurs vulnérabilités ont été découvertes dans les produits VMware. Certaines peuvent être exploitées par un attaquant pour obtenir une élévation de privilèges, compromettre la confidentialité des données ou contourner les mécanismes de sécurité.

SOLUTION :

Consulter le bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

DOCUMENTATION :

- Bulletin de sécurité VMware 36149 du 29 septembre 2025

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149

- Bulletin de sécurité VMware 36150 du 29 septembre 2025

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36150

- Référence CVE CVE-2025-41244

https://www.cve.org/CVERecord?id=CVE-2025-41244

- Référence CVE CVE-2025-41245

https://www.cve.org/CVERecord?id=CVE-2025-41245

- Référence CVE CVE-2025-41246

https://www.cve.org/CVERecord?id=CVE-2025-41246

- Référence CVE CVE-2025-41250

https://www.cve.org/CVERecord?id=CVE-2025-41250

- Référence CVE CVE-2025-41251

https://www.cve.org/CVERecord?id=CVE-2025-41251

- Référence CVE CVE-2025-41252

https://www.cve.org/CVERecord?id=CVE-2025-41252