

Agence Nationale
des Systèmes d'information
de l'état

Djibouti le, 23-08-2024

BULLETIN ALERTES

Object	Multiples vulnérabilités dans les produits VMware
Référence	1224
Date de Publication	2024-08-23
Sévérité	Elevé

IMPACT :

- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Déni de service à distance
- Exécution de code arbitraire à distance
- Injection de code indirecte à distance (XSS)
- Élévation de privilège

SYSTÈME AFFECTÉ :

- CF Deployment versions antérieures à 41.0.0
- Cflinuxfs3 versions antérieures à 0.390.0
- Cflinuxfs4 versions antérieures à 1.99.0
- Jammy Stemcells versions antérieures à 1.486
- Operations Manager Image versions 2.10.x antérieures à 2.10.75
- Operations Manager Image versions 2.7.x antérieures à 2.7.25
- Operations Manager Image versions 2.8.x antérieures à 2.8.16
- Operations Manager Image versions 3.x LTS-T antérieures à 3.0.30+LTS-T
- Operations Manager versions 2.10.x antérieures à 2.10.75
- Operations Manager versions 2.7.x antérieures à 2.7.25
- Operations Manager versions 2.8.x antérieures à 2.8.16
- Operations Manager versions 2.9.x antérieures à 2.9.12
- Operations Manager versions 3.x LTS-T antérieures à 3.0.30+LTS-T
- Platform Automation Toolkit versions 4.0.x antérieures à 4.0.13
- Platform Automation Toolkit versions 4.1.x antérieures à 4.1.13
- Platform Automation Toolkit versions 4.2.x antérieures à 4.2.8
- Platform Automation Toolkit versions 4.3.x antérieures à 4.3.5
- Platform Automation Toolkit versions 4.4.x antérieures à 4.4.32
- Platform Automation Toolkit versions 5.0.x antérieures à 5.0.25
- Platform Automation Toolkit versions 5.1.x antérieures à 5.1.2
- Tanzu Greenplum pour Kubernetes versions 1.x antérieures à 1.2.0
- Tanzu Greenplum pour Kubernetes versions 2.x antérieures à 2.0.0
- Xenial Stemcells versions antérieures à 621.969

DÉSCRIPTION :

Plusieurs vulnérabilités ont été identifiées dans les produits VMware. Certaines d'entre elles pourraient permettre à un attaquant d'exécuter du code arbitraire, d'élever ses privilèges et d'effectuer une injection de code indirecte à distance (XSS).

SOLUTION :

Mettre à jour les produits VMware.(se référer à la documentation)

DOCUMENTATION :

- Bulletin de sécurité VMware 24703 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24703>

- Bulletin de sécurité VMware 24704 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24704>

- Bulletin de sécurité VMware 24722 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24722>

- Bulletin de sécurité VMware 24724 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24724>

- Bulletin de sécurité VMware 24726 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24726>

- Bulletin de sécurité VMware 24728 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24728>

- Bulletin de sécurité VMware 24729 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24729>

- Bulletin de sécurité VMware 24730 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24730>

- Bulletin de sécurité VMware 24731 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24731>

- Bulletin de sécurité VMware 24746 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24746>

- Bulletin de sécurité VMware 24749 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24749>

- Bulletin de sécurité VMware 24750 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24750>

- Bulletin de sécurité VMware 24754 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24754>

- Bulletin de sécurité VMware 24757 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24757>

- Bulletin de sécurité VMware 24758 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24758>

- Bulletin de sécurité VMware 24759 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24759>

- Bulletin de sécurité VMware 24760 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24760>

- Bulletin de sécurité VMware 24761 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24761>

- Bulletin de sécurité VMware 24762 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24762>

- Bulletin de sécurité VMware 24763 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24763>

- Bulletin de sécurité VMware 24790 du 22 août 2024

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24790>

- CVE-2016-9840

<https://www.cve.org/CVERecord?id=CVE-2016-9840>

- CVE-2016-9841

<https://www.cve.org/CVERecord?id=CVE-2016-9841>

- CVE-2018-25032

<https://www.cve.org/CVERecord?id=CVE-2018-25032>

- CVE-2019-9511

<https://www.cve.org/CVERecord?id=CVE-2019-9511>

- CVE-2019-9513

<https://www.cve.org/CVERecord?id=CVE-2019-9513>

- CVE-2022-37434

<https://www.cve.org/CVERecord?id=CVE-2022-37434>

- CVE-2022-40735

<https://www.cve.org/CVERecord?id=CVE-2022-40735>

- CVE-2022-48622

<https://www.cve.org/CVERecord?id=CVE-2022-48622>

- CVE-2023-22655

<https://www.cve.org/CVERecord?id=CVE-2023-22655>

- CVE-2023-28746

<https://www.cve.org/CVERecord?id=CVE-2023-28746>

- CVE-2023-3164

<https://www.cve.org/CVERecord?id=CVE-2023-3164>

- CVE-2023-38575

<https://www.cve.org/CVERecord?id=CVE-2023-38575>

- CVE-2023-39368

<https://www.cve.org/CVERecord?id=CVE-2023-39368>

- CVE-2023-43490

<https://www.cve.org/CVERecord?id=CVE-2023-43490>

- CVE-2023-44487

<https://www.cve.org/CVERecord?id=CVE-2023-44487>

- CVE-2023-45733

<https://www.cve.org/CVERecord?id=CVE-2023-45733>

- CVE-2023-45745

<https://www.cve.org/CVERecord?id=CVE-2023-45745>

- CVE-2023-46103

<https://www.cve.org/CVERecord?id=CVE-2023-46103>

- CVE-2023-47855

<https://www.cve.org/CVERecord?id=CVE-2023-47855>

- CVE-2023-50387

<https://www.cve.org/CVERecord?id=CVE-2023-50387>

- CVE-2023-50868

<https://www.cve.org/CVERecord?id=CVE-2023-50868>

- CVE-2023-7104

<https://www.cve.org/CVERecord?id=CVE-2023-7104>

- CVE-2024-1013

<https://www.cve.org/CVERecord?id=CVE-2024-1013>

- CVE-2024-26256

<https://www.cve.org/CVERecord?id=CVE-2024-26256>

- CVE-2024-28182

<https://www.cve.org/CVERecord?id=CVE-2024-28182>

- CVE-2024-33599

<https://www.cve.org/CVERecord?id=CVE-2024-33599>

- CVE-2024-33600

<https://www.cve.org/CVERecord?id=CVE-2024-33600>

- CVE-2024-33601

<https://www.cve.org/CVERecord?id=CVE-2024-33601>

- CVE-2024-33602

<https://www.cve.org/CVERecord?id=CVE-2024-33602>

- CVE-2024-34064

<https://www.cve.org/CVERecord?id=CVE-2024-34064>

- CVE-2024-34397

<https://www.cve.org/CVERecord?id=CVE-2024-34397>

- CVE-2024-3651

<https://www.cve.org/CVERecord?id=CVE-2024-3651>

- CVE-2024-38428

<https://www.cve.org/CVERecord?id=CVE-2024-38428>

- CVE-2024-6387

<https://www.cve.org/CVERecord?id=CVE-2024-6387>