ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات
مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre : **Vulnérabilités dans les produits VMware**

Numéro de Référence : 21030307/19
Risque : Important
Impact : Important

Systèmes affectés

- AppDefense
- Container Service Extension
- Enterprise PKS
- Horizon
- Horizon DaaS
- Hybrid Cloud Extension
- Identity Manager
- Integrated OpenStack
- NSX for vSphere
- NSX-T Data Center
- Pulse Console
- SD-WAN Edge by VeloCloud
- SD-WAN Gateway by VeloCloud
- SD-WAN Orchestrator by VeloCloud
- Skyline Collector
- Unified Access Gateway
- vCenter Server Appliance
- vCloud Availability Appliance
- vCloud Director For Service Providers

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- vCloud Usage Meter
- vRealize Automation
- vRealize Business for Cloud
- vRealize Code Stream
- vRealize Log Insight
- vRealize Network Insight
- vRealize Operations Manager
- vRealize Orchestrator Appliance
- vRealize Suite Lifecycle Manager
- vSphere Data Protection
- vSphere Integrated Containers
- vSphere Replication

Identificateurs externes

- CVE-2019-11477, CVE-2019-11478

Bilan de la vulnérabilité

.

Plusieurs vulnérabilités ont été corrigées dans les produits VMware. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer un déni de service à distance.

Solution :

- Veuillez-vous référer aux bulletins de sécurité VMware du 02 Juillet 2019
- https://www.vmware.com/security/advisories/VMSA-2019-0010.html

Risque :

- Déni de service à distance

Références :

- Bulletin de sécurité VMware du 02 Juillet 2019
- https://www.vmware.com/security/advisories/VMSA-2019-0010.html