ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Zero-day activement exploité affectant Fortinet FortiManager
Numéro de Référence	50472410/24
Date de publication	24 Octobre 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- FortiManager versions 7.6.x antérieures à la version 7.6.1
- FortiManager versions 7.4.x antérieures à la version 7.4.5
- FortiManager versions 7.2.x antérieures à la version 7.2.8
- FortiManager versions 7.0.x antérieures à la version 7.0.13
- FortiManager versions 6.4.x antérieures à la version 6.4.15
- FortiManager versions 6.2.x antérieures à la version 6.2.13
- FortiManager Cloud versions 7.4.x antérieures à la version 7.4.5
- FortiManager Cloud versions 7.2.x antérieures à la version 7.2.8
- FortiManager Cloud versions 7.0.x antérieures à la version 7.0.13
- FortiManager Cloud versions 6.4.x

Identificateurs externes

- CVE-2024-47575

Bilan de la vulnérabilité

Fortinet annonce la disponibilité de mises à jour de sécurité permettant la correction d'un « Zero-day » affectant les versions susmentionnées de son produit FortiManager. Cette vulnérabilité est activement exploitée et elle peut permettre à un attaquant distant d'exécuter du code arbitraire et d'accéder à des informations confidentielles

Solution

Veuillez se référer au bulletin de sécurité de Fortinet pour mettre à jour vos produits.

Risques

- Accès à des données confidentielles
- Exécution de code arbitraire

Indicateurs de compromission

Logs

type=event,subtype=dvm,pri=information,desc="Device,manager,generic,information,log",user="device,...",msg="Unregistered device localhost add succeeded" device="localhost" adom="FortiManager" session_id=0 operation="Add device" performed_on="localhost" changes="Unregistered device localhost add succeeded"

type=event,subtype=dvm,pri=notice,desc="Device,Manager,dvm,log,at,notice,level",user="System",userfrom="",msg="" adom="root" session_id=0 operation="Modify device" performed_on="localhost" changes="Edited device settings (SN FMG-VMTM23017412)"

Adresses IP

45.32.41.202

104.238.141.143

158.247.199.37

45.32.63.2

Serial Number

FMG-VMTM23017412

Fichiers

/tmp/.tm

/var/tmp/.tm

Références

Bulletin de sécurité de Fortinet:

- https://www.fortiguard.com/psirt/FG-IR-24-423