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

BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits Fortinet
Numéro de Référence	47501605/24
Date de Publication	16 Mai 2024
Risque	Important
Impact	Important

Systèmes affectés

- FortiWebManager 7.2.x versions antérieures à 7.2.1
- FortiWebManager 7.0.x versions antérieures à 7.0.5
- FortiWebManager 6.3.x versions antérieures à 6.3.1
- FortiWebManager 6.2.x versions antérieures à 6.2.5
- FortiWebManager 6.0.x toutes versions
- FortiWeb 7.4.x versions antérieures à 7.4.3
- FortiWeb 7.2.x versions antérieures à 7.2.8
- FortiWeb 7.0.x versions antérieures à 7.0.9
- FortiWeb 7.0.x toutes versions
- FortiWeb 6.4.x toutes versions
- FortiWeb 6.3.x toutes versions
- FortiVoice 7.0.x versions antérieures à 7.0.2
- FortiVoice 6.4.x versions antérieures à 6.4.9
- FortiVoice 6.0.x toutes versions
- FortiSwitchManager 7.2.x versions antérieures à 7.2.3
- FortiSwitchManager 7.0.x versions antérieures à 7.0.3
- FortiSandbox 4.4.x versions antérieures à 4.4.5
- FortiSandbox 4.2.x versions antérieures à 4.2.7
- FortiSOAR cyops Connector versions antérieures à 2.1.0
- FortiSOAR 7.3.x versions antérieures à 7.3.1
- FortiSOAR 7.2.x toutes versions

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

- FortiSOAR 7.0.x toutes versions
- FortiProxy 7.4.x versions antérieures à 7.4.2
- FortiProxy 7.2.x versions antérieures à 7.2.8
- FortiProxy 7.0.x versions antérieures à 7.0.14
- FortiProxy 2.0.x toutes versions
- FortiProxy 1.2.x toutes versions
- FortiProxy 1.1.x toutes versions
- FortiProxy 1.0.x toutes versions
- FortiPortal 7.2.x versions antérieures à 7.2.2
- FortiPortal 7.0.x versions antérieures à 7.0.7
- FortiPortal 6.0.x versions antérieures à 6.0.15
- FortiPAM 1.1.x versions antérieures à 1.1.1
- FortiPAM 1.0.x toutes versions
- FortiOS 7.4.x versions antérieures à 7.4.2
- FortiOS 7.2.x versions antérieures à 7.2.8
- FortiOS 7.0.x versions antérieures à 7.0.13
- FortiOS 7.0 toutes versions
- FortiOS 6.4.x toutes versions
- FortiOS 6.2.x toutes versions
- FortiOS 6.0.x toutes versions
- FortiNAC 9.4.x versions antérieures à 9.4.5
- FortiNAC 9.2.x toutes versions
- FortiNAC 9.1.x toutes versions
- FortiNAC 8.8.x toutes versions
- FortiNAC 8.7.x toutes versions
- FortiNAC 7.2.x versions antérieures à 7.2.4
- FortiAuthenticator 6.6.x versions antérieures à 6.6.1
- FortiAuthenticator 6.5.x versions antérieures à 6.5.4
- FortiAuthenticator 6.4.x toutes versions
- FortiADC 7.4.x versions antérieures à 7.4.2
- FortiADC 7.2.x versions antérieures à 7.2.4
- FortiADC 7.1.x toutes versions
- FortiADC 7.0.x toutes versions

- FortiADC 6.2.x toutes versions

Identificateurs externes

- CVE-2023-36640 CVE-2023-40720 CVE-2023-44247 CVE-2023-45288 CVE-2023-45583 CVE-2023-45586 CVE-2023-46714 CVE-2023-48789 CVE-2023-50180 CVE-2024-21760 CVE-2024-23105 CVE-2024-23107 CVE-2024-23664 CVE-2024-23665 CVE-2024-23667 CVE-2024-23668 CVE-2024-23669 CVE-2024-23670 CVE-2024-24549 CVE-2024-26007 CVE-2024-27316 CVE-2024-27983 CVE-2024-28182 CVE-2024-30255 CVE-2024-31488 CVE-2024-31491 CVE-2024-31493 CVE-2024-3302

Bilan de la vulnérabilité

Fortinet a publié des mises à jour de sécurité pour corriger plusieurs vulnérabilités affectant les produits susmentionnés. L'exploitation réussie de ces vulnérabilités pourrait permettre à un attaquant d'exécuter du code, de causer un déni de service, de contourner la politique de sécurité et de porter atteinte à la confidentialité des données.

Solution

Veuillez se référer au bulletin de sécurité Fortinet du 14 Mai 2024 afin d'installer les nouvelles mises à jour.

Risque

- Exécution du code arbitraire à distance
- Déni de service
- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité

Annexe

Bulletins de sécurité Fortinet du 14 Mai 2024:

- https://www.fortiguard.com/psirt/FG-IR-24-120
- https://www.fortiguard.com/psirt/FG-IR-24-054
- https://www.fortiguard.com/psirt/FG-IR-24-052
- https://www.fortiguard.com/psirt/FG-IR-24-040
- https://www.fortiguard.com/psirt/FG-IR-24-021
- https://www.fortiguard.com/psirt/FG-IR-24-017
- https://www.fortiguard.com/psirt/FG-IR-23-474
- https://www.fortiguard.com/psirt/FG-IR-23-465
- https://www.fortiguard.com/psirt/FG-IR-23-433
- https://www.fortiguard.com/psirt/FG-IR-23-420
- https://www.fortiguard.com/psirt/FG-IR-23-415
- https://www.fortiguard.com/psirt/FG-IR-23-406
- https://www.fortiguard.com/psirt/FG-IR-23-282

- https://www.fortiguard.com/psirt/FG-IR-23-225
- https://www.fortiguard.com/psirt/FG-IR-23-222
- https://www.fortiguard.com/psirt/FG-IR-23-195
- https://www.fortiguard.com/psirt/FG-IR-23-191
- https://www.fortiguard.com/psirt/FG-IR-23-137