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	39630501/23
Date de Publication	05 Janvier 2023
Risque	Important
Impact	Important

Systèmes affectés

- FortiADC version 7.0.0 à 7.0.1
- FortiADC version 6.2.0 à 6.2.3
- FortiADC version 6.1.0 à 6.1.6
- FortiADC version 6.0.0 à 6.0.4
- FortiADC version 5.4.0 à 5.4.5
- FortiManager version 7.0.0 à 7.0.1
- FortiManager version 6.4.0 à 6.4.7
- FortiManager version 6.2.0 à 6.2.8
- FortiWeb version 7.0.0 à 7.0.2
- FortiWeb version 6.4.0 à 6.4.2
- FortiWeb version 6.3.6 à 6.3.20
- FortiPortal version 6.0.0 à 6.0.11
- FortiPortal 5.3 all versions
- FortiPortal 5.2 all versions
- FortiPortal 5.1 all versions
- FortiPortal 5.0 all versions
- FortiTester version 7.1.0
- FortiTester version 7.0 all versions
- FortiTester version 4.0.0 à 4.2.0
- FortiTester version 2.3.0 à 3.9.1

Identificateurs externes

- CVE-2022-43931, CVE-2022-35845, CVE-2022-41336, CVE-2022-45857

Bilan de la vulnérabilité

Fortinet a publié un avis de sécurité pour corriger plusieurs vulnérabilités dans les produits susmentionnés. L'exploitation de ces failles peut permettre à un attaquant distant d'exécuter

du code ou des commandes arbitraires non autorisés via des requêtes HTTP spécifiquement conçues.

Solution

Veuillez se référer au bulletin de sécurité Fortinet du 03 Janvier 2023 afin d'installer les nouvelles mises à jour.

Risque

- Exécution du code arbitraire,

Annexe

Bulletins de sécurité Fortinet du 03 Janvier 2023**:**

- https://www.fortiguard.com/psirt/FG-IR-22-061
- https://www.fortiguard.com/psirt/FG-IR-22-371
- https://www.fortiguard.com/psirt/FG-IR-22-250
- https://www.fortiguard.com/psirt/FG-IR-22-313
- https://www.fortiguard.com/psirt/FG-IR-22-274