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	38990311/22
Date de Publication	03 Novembre 2022
Risque	Important
Impact	Important

Systèmes affectés

- FortiTester versions 7.2.x antérieures à 7.2.0
- FortiTester versions 7.1.x antérieures à 7.1.1
- FortiTester versions 4.2.x antérieures à 4.2.1
- FortiTester versions 3.9.x antérieures à 3.9.2
- FortiSOAR versions 7.2.x antérieures à 7.2.3
- FortiSIEM versions 6.5.x antérieures à 6.5.0
- FortiOS versions 7.2.x antérieures à 7.2.2
- FortiOS versions 7.0.x antérieures à 7.0.8
- FortiOS versions 6.4.x antérieures à 6.4.10
- FortiManager versions 7.0.x antérieures à 7.0.5
- FortiManager versions 6.4.x antérieures à 6.4.9
- FortiMail versions 7.2.x antérieures à 7.2.1
- FortiMail versions 7.0.x antérieures à 7.0.4
- FortiMail versions 6.4.x antérieures à 6.4.7
- FortiEDR CollectorWindows versions 5.2.x.x antérieures à 5.2.0.2288
- FortiEDR CollectorWindows versions 5.0.x.x antérieures à 5.0.3.912
- FortiDeceptor versions 4.2.x antérieures à 4.2.1
- FortiDeceptor versions 4.1.x antérieures à 4.1.2
- FortiDeceptor versions 4.0.x antérieures à 4.0.3
- FortiClientMac versions 7.0.x antérieures à 7.0.6
- FortiAnalyzer versions 7.0.x antérieures à 7.0.5

- FortiAnalyzer versions 6.4.x antérieures à 6.4.9
- FortiADC versions 7.1.x antérieures à 7.1.1
- FortiADC versions 7.0.x antérieures à 7.0.3
- FortiADC versions 6.2.x antérieures à 6.2.4
- AV engine versions 6.4.x antérieures à 6.4.275
- AV engine versions 6.2.x antérieures à 6.2.169

Identificateurs externes

- CVE-2022-26122 CVE-2022-38374 CVE-2022-35851 CVE-2022-38381 CVE-2022-33878 CVE-2022-38373 CVE-2022-39949 CVE-2022-39945 CVE-2022-39950 CVE-2022-30307 CVE-2022-38380 CVE-2022-35842 CVE-2022-26119 CVE-2022-42473 CVE-2022-33870

Bilan de la vulnérabilité

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

Solution

Veuillez se référer au bulletin de sécurité Fortinet du 01 Novembre 2022 afin d'installer les nouvelles mises à jour.

Risque

- Exécution du code arbitraire
- Atteinte à la confidentialité de données
- Contournement de la politique de sécurité

Annexe

Bulletins de sécurité Fortinet du 01 Novembre 2022 :

- https://www.fortiguard.com/psirt/FG-IR-22-074
- https://www.fortiguard.com/psirt/FG-IR-22-232
- https://www.fortiguard.com/psirt/FG-IR-22-314
- https://www.fortiguard.com/psirt/FG-IR-22-234
- https://www.fortiguard.com/psirt/FG-IR-22-246
- https://www.fortiguard.com/psirt/FG-IR-22-331
- https://www.fortiguard.com/psirt/FG-IR-22-218
- https://www.fortiguard.com/psirt/FG-IR-22-066
- https://www.fortiguard.com/psirt/FG-IR-21-228
- https://www.fortiguard.com/psirt/FG-IR-22-228

- https://www.fortiguard.com/psirt/FG-IR-22-174
- https://www.fortiguard.com/psirt/FG-IR-22-223
- https://www.fortiguard.com/psirt/FG-IR-22-064
- https://www.fortiguard.com/psirt/FG-IR-22-216
- https://www.fortiguard.com/psirt/FG-IR-22-070