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 critiques dans les produits Fortinet
Numéro de Référence	40422002/23
Date de Publication	20 Février 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- FortiADC versions 5.x à 6.2.x antérieures à 6.2.4
- FortiADC versions 7.0.x antérieures à 7.0.2
- FortiAnalyzer versions 6.x antérieures à 6.4.9
- FortiAnalyzer versions 7.0.x antérieures à 7.0.5
- FortiAnalyzer versions 7.2.x antérieures à 7.2.2
- FortiAuthenticator versions 5.x à 6.0.x antérieures à 6.0.5
- FortiAuthenticator versions 6.1.x antérieures à 6.1.1
- FortiExtender versions 3.x antérieures à 3.2.4
- FortiExtender versions 3.3.x antérieures à 3.3.3
- FortiExtender versions 4.0.x antérieures à 4.0.3 (version à venir)
- FortiExtender versions 4.1.x antérieures à 4.1.9 (version à venir)
- FortiExtender versions 4.2.x antérieures à 4.2.5 (version à venir)
- FortiExtender versions 5.3.x antérieures à 7.0.4
- FortiGate versions antérieures à 6.4.2
- FortiNAC-F versions antérieures à 7.2.0
- FortiNAC versions 8.x à 9.4.x antérieures à 9.4.2
- FortiOS versions 6.0.x à 7.0.x antérieures à 7.0.9
- FortiOS versions 7.2.x antérieures à 7.2.4
- FortiPortal versions 7.0.x antérieures à 7.0.3
- FortiProxy versions 1.x à 7.0.x antérieures à 7.0.8
- FortiProxy versions 7.2.x antérieures à 7.2.2

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

- FortiSandbox versions 3.2.x à 4.x antérieures à 4.2.0
- FortiSwitchManager versions 7.0.x antérieures à 7.0.1
- FortiSwitchManager versions 7.2.x antérieures à 7.2.1
- FortiSwitch versions 6.x antérieures à 6.4.11
- FortiSwitch versions 7.0.x antérieures à 7.0.4
- FortiWAN versions 4.x antérieures à 4.5.10
- FortiWeb versions 5.x à 7.x antérieures à 7.0.5
- FortiADC 5.1 all versions
- FortiADC 5.0 all versions

Identificateurs externes

- CVE-2021-42756 , CVE-2021-42761 , CVE-2021-43074 , CVE-2022-22302 , CVE-2022-26115 , CVE-2022-27482 , CVE-2022-27489 , CVE-2022-29054 , CVE-2022-30299 , CVE-2022-30300 , CVE-2022-30303 , CVE-2022-30304 , CVE-2022-30306 , CVE-2022-33869 , CVE-2022-33871 , CVE-2022-38375 , CVE-2022-38376 , CVE-2022-38378 , CVE-2022-39948 , CVE-2022-39952 , CVE-2022-39954 , CVE-2022-40675 , CVE-2022-40677 , CVE-2022-40678 , CVE-2022-40683 , CVE-2022-41335 , CVE-2022-42472 , CVE-2022-43954 , CVE-2023-22636 , CVE-2023-22638 , CVE-2023-23777 , CVE-2023-23778 , CVE-2023-23779 , CVE-2023-23780 , CVE-2023-23781 , CVE-2023-23782 , CVE-2023-23783 , CVE-2023-23784 , CVE-2023-25602

Bilan de la vulnérabilité

Fortinet a publié des mises à jour de sécurité pour corriger plusieurs vulnérabilités critiques affectant les produits susmentionnés. L'exploitation réussie de ces vulnérabilités pourrait permettre à un attaquant de réussir une élévation de privilèges, de contourner la politique de sécurité, de porter atteinte à la confidentialité et d'exécuter du code arbitraire à distance.

Solution

Veuillez se référer au bulletin de sécurité Fortinet du 10 Octobre 2022 afin d'installer les nouvelles mises à jour.

Risque

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

Annexe

Bulletins de sécurité Fortinet du 10 Octobre 2022:

- https://www.fortiguard.com/psirt/FG-IR-22-377