CYBER DEFENSE AFRICA : ANNONCE DE SÉCURITÉ **Date** : 19/12/2024

Type de Contenu	Description
Titre	***Vulnérabilités critiques de Fortinet permettant aux attaquants d'injecter des codes à distance et de récupérer des fichiers sensibles (CVE-2024-48889 & CVE-2023-34990)***
ID	*202412/AS/93*
Code TLP	*Green*
Niveau de risque	***Critique***
Application et service affectés	• *FortiManager, ainsi que certains anciens modèles de FortiAnalyzer tels que 1000E, 3000F et 3700G* • *FortiWLM (Wireless Manager)*
Version / Edition	*Versions affectées :* • *FortiManager 6.4* ***(6.4.10 à 6.4.14) ;*** *7.0* ***(7.0.5 à 7.0.12) ;*** *7.2* ***(7.2.3 à 7.2.7) ;*** *7.4* ***(7.4.0 à 7.4.4) ; et*** *7.6* ***(7.6.0)*** • *FortiManager Cloud 7.0* ***(7.0.1 à 7.0.12) ;*** *7.2* ***(7.2.1 à 7.2.7****) et 7.4* ***(7.4.1 à 7.4.4)*** • *FortiWLM 8.5* ***(8.5.0 à 8.5.4)*** *et 8.6* ***(8.6.0 à 8.6.5)***
Plateforme	***FortiManager; FortiAnalyzer et FortiWLM***
Mise à jour	*Vulnérabilités corrigées dans les versions :* • *FortiManager 6.4.15; 7.0.13; 7.4.5 et 7.6.1 ou versions ultérieures* • *FortiManager Cloud 7.0.13 ; 7.2.8 et 7.4.5 ou versions ultérieures.* • *FortiWLM 8.6.6 ou ou versions ultérieures.*
Résumé	***Fortinet a publié un avis de sécurité urgent concernant deux vulnérabilités critiques affectant ses produits FortiManager et FortiWLM***
Impacts	- ***Exécution de code arbitraire à distance*** - ***Accès en lecture et non autorisé à des fichiers sensibles*** - ***Fuites de données et de violations potentielles d'informations sensibles.*** - ***Vol et exfiltration d'informations sensibles et confidentielles***
Description Détaillée	*Fortinet, un acteur majeur des solutions de cybersécurité, a publié un avis de sécurité urgent concernant deux vulnérabilités critiques affectant ses produits FortiManager et FortiWLM.* *La première vulnérabilité identifiée sous* ***CVE-2024-48889****, a une sévérité critique et affecte* ***FortiManager*** *ainsi que certains anciens modèles de* ***FortiAnalyzer*** *tels que 1000E, 1000F, 2000E, 3000E, 3000F, 3000G, 3500E, 3500F, 3500G, 3700F, 3700G et 3900E s'ils sont configurés avec les paramètres suivants :* ***config system global*** ***set fmg-status enable*** ***end.*** *Elle permet à des attaquants authentifiés d'exécuter des commandes arbitraires à distance via des requêtes FGFM (Fortinet secure communication protocol) spécialement*

	conçues. *La deuxième vulnérabilité critique (**CVE-2023-34990)**, a été découverte dans le **FortiWLM (Wireless Manager)** et permet à des attaquants distants non authentifiés de récupérer des fichiers sensibles via la « relative path traversal » tout en posant des risques de fuites de données et de violations potentielles d'informations sensibles.*
Recommandations	1. ***Solutions de mise à jour pour CVE-2024-48889 :*** - *Mettre à jour les versions **FortiManager** affectées vers les versions 6.4.15; 7.0.13; 7.4.5 et 7.6.1 ou ultérieures* - *Mettre à jour les versions **FortiManager Cloud** affectées vers les versions 7.0.13 ; 7.2.8 et 7.4.5 ou ultérieures.* - *Appliquer les mises à jour sur les anciens modèles de **FortiAnalyzer** tels que 1000E, 1000F, 2000E, 3000E, 3000F, 3000G, 3500E, 3500F, 3500G, 3700F, 3700G et 3900E s'ils sont configurés avec les paramètres : (config system global, set fmg-status enable, end).* 2. ***Solutions de mise à jour pour CVE-2023-34990 :*** - Mettre à jour ***FortiWLM 8.6*** *(8.6.0 à 8.6.5) vers* la version *8.6.6 ou ultérieure* - *Mettre à jour **FortiWLM 8.5** (8.5.0 à 8.5.4) vers la version 8.5.5 ou ultérieure*
Indicateurs de Compromission	***Adresses IP :*** - *45.32.41.202* - *104.238.141.143* - *158.247.199.37* - *45.32.63.2* - *80.66.196.199* - *198.199.122.22* - *142.93.177.233* - *195.85.114.78* - *172.232.167.68* ***Numéro de série :*** - *FMG-VMTM23017412* - *FMG-VMTM19008093* - *FGVMEVWG8YMT3R63* ***Fichiers :*** - */tmp/.tm* - */var/tmp/.tm* *Il est à noter que les codes d'identification de fichier peuvent ne pas apparaître dans tous les cas.*
Liens pour plus de détails	- *https://fortiguard.fortinet.com/psirt/FG-IR-24-425* - *https://www.cve.org/CVERecord?id=CVE-2024-48889*