CYBER DEFENSE AFRICA : ANNONCE DE SÉCURITÉ **Date** : 16/01/2025

Type de Contenu	Description
Titre	***Vulnérabilité critique d'accès non autorisé dans FortiOS et FortiProxy***
ID	*2025/AS/02*
Code TLP	*Green*
Niveau de Risque	***Critique***
Application et service affectés	*FortiOS et FortiProxy*
Version / Edition	*FortiOS 7.0.0 à 7.0.16 et FortiProxy 7.0.0 à 7.0.19 ainsi que 7.2.0 à 7.2.12*
Plateforme	***Fortinet***
Mise à jour	*FortiOS 7.0 : Versions 7.0.0 à 7.0.16 – Mettez à jour vers 7.0.17 ou supérieure.* *FortiProxy 7.2 : Versions 7.2.0 à 7.2.12 – Mettez à jour vers 7.2.13 ou supérieure.* *FortiProxy 7.0 : Versions 7.0.0 à 7.0.19 – Mettez à jour vers 7.0.20 ou supérieure.*
Résumé	*La vulnérabilité découverte dans FortiOS et FortiProxy permet à un attaquant distant de bypasser l'authentification et d'obtenir des privilèges de super-administrateur via une faille dans le module WebSocket de Node.js. Elle est activement exploitée depuis* ***novembre 2024****.*
Impacts	***Prise de contrôle complète du système, Accès non autorisé aux données sensibles***
Description Détaillée	*La vulnérabilité* ***CVE-2024-55591*** *est un contournement d'authentification de type* ***CWE-288*** *affectant* ***FortiOS*** *et* ***FortiProxy****. Elle permet à un attaquant distant non authentifié de contourner le mécanisme d'authentification en exploitant une faille dans le module WebSocket de* ***Node.js****. En envoyant des requêtes malveillantes, l'attaquant peut obtenir des privilèges de* ***super-administrateur*** *sur le système, ce qui lui permet de prendre le contrôle complet du dispositif. Cette faille est activement exploitée depuis* ***novembre 2024*** *et présente un* ***risque élevé****, avec un score* ***CVSSv3 de 9.6****. L'exploitation de cette vulnérabilité ne nécessite aucune interaction de l'utilisateur et peut se produire à distance, ce qui accentue son danger. Fortinet a publié un correctif pour corriger cette vulnérabilité et protéger les systèmes affectés.*
Recommandations	***Mettre à jour immédiatement les versions de FortiOS et FortiProxy vulnérables vers les versions corrigées***
Indicateurs de Compromission	*NA*
Liens pour plus de détails	*https://www.fortiguard.com/psirt/FG-IR-24-535*