Type de Contenu	Description
Titre	***Vulnérabilité critique (CVE-2024-48887) de FortiSwitch GUI***
ID	*202504/AS/24*
Code TLP	*Green*
Niveau de Risque	***Critique***
Application et service affectés	*Fortinet/ FortiSwitch GUI (Interface Graphique Utilisateur)*
Version / Edition	• *FortiSwitch 7.6 (7.6.0)* • *FortiSwitch 7.4 (7.4.0 à 7.4.4)* • *FortiSwitch 7.2 (7.2.0 à 7.2.8)* • *FortiSwitch 7.0 (7.0.0 à 7.0.10)* • *FortiSwitch 6.4 (6.4.0 à 6.4.14)*
Plateforme	***Fortinet***
Mise à jour	*FortiSwitch 7.6.1; 7.4.5 ; 7.2.9; 7.0.11 ; 6.4.15 ou versions ultérieures*
Résumé	*Fortinet a identifié une vulnérabilité critique dans l'interface graphique de FortiSwitch, permettant à un attaquant de modifier le mot de passe administrateur à distance, sans authentification.* ***Une mise à jour immédiate est impérative pour éviter toute compromission.***
Impacts	• ***Élévation des privilèges utilisateur,*** • ***Exécution des commandes arbitraires,*** • ***Prise de contrôle complète du système,*** • ***Accès non autorisé aux données et configuration sensibles .***
Détails Techniques	*Fortinet a publié des correctifs de sécurité pour remédier à une vulnérabilité critique identifiée sous le code* ***CVE-2024-48887****, affectant l'interface graphique (GUI) des commutateurs FortiSwitch.* *Cette faille permet à un attaquant distant, non authentifié, de modifier les mots de passe d'administration, y compris celui de l'utilisateur* ***admin****, via des requêtes spécialement conçues.* *Avec un* ***score CVSS de 9,3 sur 10****, cette vulnérabilité est classée comme* ***critique*** *en raison du risque élevé de compromission complète du système.* *Les versions impactées sont les suivantes :* • ***FortiSwitch 7.6.0*** *→ correctif disponible à partir de la version* ***7.6.1*** • ***FortiSwitch 7.4.0 à 7.4.4*** *→ correctif à partir de la version* ***7.4.5*** • ***FortiSwitch 7.2.0 à 7.2.8*** *→ correctif à partir de la version* ***7.2.9*** • ***FortiSwitch 7.0.0 à 7.0.10*** *→ correctif à partir de la version* ***7.0.11***

	• ***FortiSwitch 6.4.0 à 6.4.14*** → *correctif à partir de la version* ***6.4.15***
Recommandations	**Recommandations de Sécurité** ***1. Mise à jour corrective (solution principale)*** *Il est fortement recommandé de procéder sans délai à la mise à jour des versions vulnérables de FortiSwitch vers les versions corrigées ci-dessous :* • ***FortiSwitch 7.6.0*** → *mettre à jour vers* ***7.6.1*** *ou version ultérieure* • ***FortiSwitch 7.4.0 à 7.4.4*** → *mettre à jour vers* ***7.4.5*** *ou version ultérieure* • ***FortiSwitch 7.2.0 à 7.2.8*** → mettre à jour vers ***7.2.9 ou version ultérieure*** • ***FortiSwitch 7.0.0 à 7.0.10*** → mettre à jour vers ***7.0.11 ou version ultérieure*** • ***FortiSwitch 6.4.0 à 6.4.14*** → mettre à jour vers ***6.4.15 ou version ultérieure*** **2. Mesures de contournement (si la mise à jour n'est pas immédiatement possible)** En cas d'impossibilité de mise à jour immédiate, appliquez les mesures de mitigation suivantes afin de réduire les risques : • ***Désactiver l'accès HTTP/HTTPS aux interfaces d'administration*** • ***Restreindre l'accès au système aux seuls hôtes de confiance pour limiter les connexions non autorisées*** *(Consultez la documentation officielle Fortinet pour le script de configuration recommandé.)*
Indicateurs de Compromission	*N/A*
Liens pour plus de détails	*https://fortiguard.fortinet.com/psirt/FG-IR-24-435*