Type de Contenu	Description
Titre	***Vulnérabilité critique (CVE-2025-32756) affectant plusieurs produits de Fortinet***
ID	*202505/AS/28*
Code TLP	*Green*
Niveau de Risque	***Critique***
Application et service affectés	*FortiMail, FortiCamera, FortiNDR, FortiRecorder et FortiVoice*
Version / Edition	• *FortiVoice : versions 6.4.0 à 6.4.10, 7.0.0 à 7.0.6, et 7.2.0* • *FortiMail : versions 7.0.0 à 7.0.8, 7.2.0 à 7.2.7, 7.4.0 à 7.4.4, et 7.6.0 à 7.6.2* • *FortiNDR : versions 7.0.0 à 7.0.6, 7.2.0 à 7.2.4, 7.4.0 à 7.4.7, et 7.6.0* • *FortiRecorder : versions 6.4.0 à 6.4.5, 7.0.0 à 7.0.5, et 7.2.0 à 7.2.3* • *FortiCamera : toutes les versions de 1.1, 2.0, et 2.1.0 à 2.1.3*
Plateforme	***Fortinet***
Mise à jour	*Versions corrigées /versions récentes*
Résumé	*Une vulnérabilité critique actuellement en cours d'exploitation affecte plusieurs produits Fortinet*
Impacts	• ***Exécution des commandes arbitraires,*** • ***Élévation des privilèges utilisateur,*** • ***Prise de contrôle complète du système,*** • ***Accès non autorisé aux données sensibles.***
Détails Techniques	*Fortinet a publié des correctifs pour la vulnérabilité critique CVE-2025-32756, une faille de type dépassement de tampon basé sur la pile (stack-based buffer overflow) qui affecte plusieurs de ses produits. Cette vulnérabilité permet à un attaquant distant non authentifié d'exécuter du code arbitraire via des requêtes HTTP spécialement conçues.* *Elle est activement exploitée, notamment contre des systèmes **FortiVoice**, avec des tentatives de suppression des journaux système, l'activation du mode débogage **fcgi** pour capturer des informations d'identification, ainsi que l'exécution de commandes arbitraires.* *Elle possède un **score CVSS critique de 9,8 sur 10**, en raison du risque élevé de compromission complète du système et de son exploitation active dans des cas d'attaques obervées.* *Des versions corrigées et recommandées par Fortinet sont disponibles :* ***FortiVoice*** • ***6.4.x** → mettre à jour vers **6.4.11** ou version ultérieure* • ***7.0.x** → mettre à jour vers **7.0.7** ou version ultérieure*

	• ***7.2.x*** → *mettre à jour vers* ***7.2.1*** *ou version ultérieure* ***FortiMail*** • ***7.0.x*** → *mettre à jour vers* ***7.0.9*** *ou version ultérieure* • ***7.2.x*** → *mettre à jour vers* ***7.2.8*** *ou version ultérieure* • ***7.4.x*** → *mettre à jour vers* ***7.4.5*** *ou version ultérieure* • ***7.6.x*** → *mettre à jour vers* ***7.6.3*** *ou version ultérieure* ***FortiNDR*** • ***7.0.x*** → *mettre à jour vers* ***7.0.7*** *ou version ultérieure* • ***7.2.x*** → *mettre à jour vers* ***7.2.5*** *ou version ultérieure* • ***7.4.x*** → *mettre à jour vers* ***7.4.8*** *ou version ultérieure* • ***7.6.x*** → *mettre à jour vers* ***7.6.1*** *ou version ultérieure* ***FortiRecorder*** • ***6.4.x*** → *mettre à jour vers* ***6.4.6*** *ou version ultérieure* • ***7.0.x*** → *mettre à jour vers* ***7.0.6*** *ou version ultérieure* • ***7.2.x*** → *mettre à jour vers* ***7.2.4*** *ou version ultérieure* ***FortiCamera*** • ***2.1.x*** → *mettre à jour vers* ***2.1.4*** *ou version ultérieure* • ***2.0*** *et* ***1.1*** → *migrer vers une version corrigée*
Recommandations	1. ***Appliquer immédiatement les correctifs :*** *Mettre à jour tous les produits affectés vers les versions corrigées mentionnées ci-dessus.* 2. ***Désactiver temporairement l'interface d'administration HTTP/HTTPS :*** *si la mise à jour immédiate n'est pas possible, désactivez cette interface pour réduire les risques.* 3. ***Surveiller les activités suspectes :*** *analysez les journaux pour détecter toute activité inhabituelle ou non autorisée.*
Indicateurs de Compromission (IoC)	• *198.105.127.124* • *43.228.217.173* • *43.228.217.82* • *156.236.76.90* • *218.187.69.244* • *218.187.69.59* *Il est recommandé de vérifier la présence de ces IoC dans vos systèmes.*
Liens pour plus de détails	*https://fortiguard.fortinet.com/psirt/FG-IR-25-254*