Type de Contenu	Description
Titre	***Des groupes de pirates ont accédé à plus de 20 000 systèmes FortiGate de Fortinet dans le monde entier en exploitant une faille de sécurité critique connue entre 2022-2023 et sous le nom de CVE-2022-42475 (score CVSS : 9,8). Cette vulnérabilité permet l'exécution de code à distance.***
ID	*202406/AS/05*
Code TLP	*Green*
Niveau de Risque	***Critique***
Application et service affectés	***La vulnérabilité CVE-2022-42475 affecte les systèmes utilisant FortiOS, le système d'exploitation développé par Fortinet pour ses appliances de sécurité réseau, notamment les pare-feu FortiGate. Cette vulnérabilité est une faille critique dans le SSL-VPN de FortiOS***
Version/Edition	*Versions de FortiOS affectées :* • *FortiOS 7.2.0 à 7.2.2* • *FortiOS 7.0.0 à 7.0.8* • *FortiOS 6.4.0 à 6.4.10* • *FortiOS 6.2.0 à 6.2.11* • *FortiOS 6.0.0 à 6.0.16*
Plateforme	***FortiOS***
Mise à jour	*Fortinet a publié des mises à jour pour corriger cette vulnérabilité. Les administrateurs doivent mettre à jour leurs systèmes FortiOS vers les versions corrigées suivantes :* 1. *FortiOS 7.2.3 et versions ultérieures* 2. *FortiOS 7.0.9 et versions ultérieures* 3. *FortiOS 6.4.11 et versions ultérieures* 4. *FortiOS 6.2.12 et versions ultérieures* 5. *FortiOS 6.0.17 et versions ultérieures*
Résumé	*La vulnérabilité permet à un attaquant distant non authentifié de mener une attaque contre un utilisateur.*
Impacts	***Permet à un attaquant distant non authentifié d'exécuter du code arbitraire ou de provoquer un déni de service (DoS) sur le système affecté.***
Description Détaillée	*Identifiée sous le nom de **CVE-2022-42475** avec un score CVSS de 9.8 (gravité Critique), la vulnérabilité est une faille critique dans le SSL-VPN de FortiOS.* *Il s'agit d'une vulnérabilité de dépassement de tampon basée sur le tas dans le service **SSL-VPN** de FortiOS.* *Elle permet à un attaquant distant non authentifié d'exécuter du code arbitraire ou de provoquer un déni de service (DoS) sur le système affecté.* *Le vecteur d'attaque principal utilisé est l'accès réseau via le service **SSL-VPN.***

Solutions	*Appliquer immédiatement les mises à jour fournies par Fortinet.* *Restreindre l'accès au service SSL-VPN à partir de réseaux de confiance uniquement.* *Activer les fonctionnalités de journalisation et surveiller les activités suspectes sur les systèmes FortiGate.*
Liens pour plus de détails	https://nvd.nist.gov/vuln/detail/CVE-2022-42475 https://www.fortiguard.com/psirt https://www.rapid7.com/blog/post/2022/12/12/cve-2022-42475-unauthenticated-remote-code-execution-vulnerability-in-fortios-exploitation-reported/