AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre de Réponse aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SÉCURITÉ

Fortinet2Shell : exécution de code à distance dans FortiClient

Contenu

I. Contexte 3
II. Vulnérabilité identifiée 3
Versions affectées et corrigées 4
III. Vecteur d'attaque 4
IV. Menaces actives 4
V. Exposition de l'Afrique et du Cameroun 5
VI. Conclusion et actions recommandées 5
VII. Références 6

I. Contexte

Le 10 novembre 2026, Fortinet a publié l'avis de sécurité FG-IR-26-194 relatif à une vulnérabilité critique affectant FortiClient, son client de sécurité et VPN installé sur les postes Windows et macOS. La faille est référencée CVE-2026-121529 et présente un score CVSS v3.1 de 9.1 (Critique) selon Fortinet.

La vulnérabilité a été découverte par le chercheur Kevin Joensen de Baldur Security lors de recherches internes, qui l'a baptisée « Fortinet2Shell ». Elle permet à un attaquant distant, sans aucune authentification, d'exécuter du code arbitraire sur le poste d'un utilisateur qui visite simplement une page web malveillante.

II. Vulnérabilité identifiée

La faille est une erreur de validation d'origine (CWE 346) dans un point de terminaison API local exposé par FortiClient. Sa cause profonde est une configuration CORS (Cross Origin Resource Sharing) trop permissive : le service local de FortiClient accorde à tort sa confiance aux requêtes provenant de n'importe quelle page web ouverte dans le navigateur.

CVE	CVE-2026-121529
Nom de code	Fortinet2Shell
Avis Fortinet	FG-IR-26-194
Type	Erreur de validation d'origine (CWE 346), mauvaise configuration CORS
Impact	Exécution de code à distance sans authentification
Score CVSS v3.1	**9.1 Critique**
Interaction utilisateur	Visite d'une page web malveillante
Date de publication	10 novembre 2026
Contournement	Aucun, mise à jour obligatoire

Versions affectées et corrigées

Les versions suivantes sont affectées. La version 8.0 des trois produits ainsi que FortiClient Mac 7.2 ne sont pas concernées.

Produit	Versions affectées	Versions corrigées
FortiClient Mac 7.4	7.4.0 à 7.4.7	7.4.8 ou ultérieure
FortiClient Windows 7.4	7.4.0 à 7.4.7	7.4.8 ou ultérieure
FortiClient Windows 7.2	7.2.0 à 7.2.14	7.2.15 ou ultérieure
FortiClient Windows PAM 7.4	7.4.0 à 7.4.7	7.4.8 ou ultérieure
FortiClient Windows PAM 7.2	7.2.0 à 7.2.14	7.2.15 ou ultérieure
FortiClient 8.0 et FortiClient Mac 7.2	Non affectés	Sans objet

III. Vecteur d'attaque

L'exploitation se déroule comme suit :

- L'attaquant attire la victime vers une page web malveillante (courriel d'hameçonnage, lien partagé sur les réseaux sociaux ou messageries, site compromis ou publicité malveillante).
- Des scripts de la page envoient silencieusement des requêtes au service local FortiClient en écoute sur la machine de la victime (port 9191 signalé par les chercheurs).
- En raison de la mauvaise configuration CORS, le service accepte ces requêtes comme légitimes et exécute les commandes ou le code fournis par l'attaquant.
- L'attaquant obtient l'exécution de code sur le poste avec les privilèges du service FortiClient, ce qui peut conduire à la prise de contrôle totale du poste, au vol des identifiants VPN et à des déplacements latéraux dans le réseau interne.

La seule interaction requise de l'utilisateur est le chargement de la page. Aucun téléchargement, aucun clic sur une pièce jointe et aucune saisie d'identifiants ne sont nécessaires. Le chercheur rapporte une exploitation fiable sur les déploiements FortiClient avec FortiPAM activé.

IV. Menaces actives

À la date de publication, Fortinet ne signale aucune exploitation confirmée dans la nature. Toutefois, plusieurs sources de renseignement sur la menace indiquent que les détails techniques sont publics, qu'une preuve de concept est disponible et que des capteurs de type honeypot ont déjà enregistré une activité liée.

Les produits Fortinet sont une cible constante des groupes de rançongiciels et des acteurs étatiques, qui ont à plusieurs reprises exploité des vulnérabilités Fortinet quelques jours après leur divulgation. L'exploitation de Fortinet2Shell est donc attendue à très court terme, notamment au travers de campagnes d'hameçonnage.

V. Exposition de l'Afrique et du Cameroun

FortiClient est largement déployé en Afrique, et au Cameroun en particulier, comme client VPN d'accès distant des pare feux FortiGate utilisés par les administrations publiques, les banques, les établissements de microfinance, les opérateurs de télécommunications et les grandes entreprises.

Les postes équipés de FortiClient sont généralement ceux des responsables, des administrateurs et du personnel en télétravail, qui disposent d'accès privilégiés aux systèmes d'information internes. La compromission d'un seul de ces postes peut offrir à un attaquant un point d'entrée dans le réseau de toute une structure. Les campagnes d'hameçonnage déjà en circulation sur les plateformes de messagerie nationales rendent ce vecteur particulièrement réaliste dans notre contexte.

VI. Conclusion et actions recommandées

Fortinet2Shell est une vulnérabilité critique qui transforme une simple visite de page web en compromission totale du poste de l'utilisateur. Compte tenu de la large utilisation de FortiClient au sein des structures nationales, le CIRT recommande vivement les actions suivantes :

1. Mettre à jour immédiatement FortiClient Windows et Mac 7.4 vers la version 7.4.8 ou ultérieure, et FortiClient Windows 7.2 vers la version 7.2.15 ou ultérieure, ou migrer vers la branche 8.0.
2. Utiliser FortiClient EMS (lorsqu'il est disponible) pour inventorier l'ensemble des postes et confirmer que chaque installation a été mise à jour.
3. Traiter en priorité les postes des responsables, des administrateurs informatiques et du personnel en télétravail, ainsi que les machines sur lesquelles FortiPAM est activé.
4. Rechercher les postes exposant localement le port 9191 ou exécutant le processus FortiVRS.exe, et vérifier leurs versions.
5. Renforcer le filtrage web et bloquer l'accès aux domaines récemment enregistrés ou non catégorisés pendant la période de déploiement des correctifs.
6. Surveiller les alertes EDR et SIEM relatives à des processus enfants ou des connexions réseau anormales initiés par les processus FortiClient.
7. Sensibiliser les utilisateurs à ne pas ouvrir de liens inconnus reçus par courriel, SMS ou messageries, et signaler tout incident suspect au CIRT.

Pour tout incident ou toute demande d'assistance, contactez le CIRT via ses canaux habituels.

VII. Références

- Fortinet PSIRT, avis FG-IR-26-194 : fortiguard.fortinet.com
- Fiche CVE-2026-121529 : www.cve.org
- GBHackers, Fortinet2Shell Vulnerability, 11 novembre 2026 : gbhackers.com
- Cybersecurity News, Critical Fortinet2Shell Vulnerability, 11 novembre 2026 : cybersecuritynews.com