Gestion des vulnérabilités : FBI, CISA et Fortinet alertent

La menace est élevée. Des vulnérabilités connues dans FortiOS, le système d'exploitation de Fortinet embarqué dans des appliances (FortiGate), sont exploitées par des attaquants. Et ce pour accéder aux réseaux de services gouvernementaux et commerciaux.

Le Bureau fédéral d'enquête (FBI) et l'Agence américaine de sécurité des infrastructures et de cybersécurité (CISA) ont publié une alerte de sécurité à ce sujet.

Trois failles sont concernées :

C'est notamment le cas de la vulnérabilité CVE-2018-13379 qui affecte les systèmes FortiOS lorsque le service VPN SSL est activé. Par ce biais, des attaquants non authentifiés peuvent accéder aux fichiers systèmes via des requêtes HTTP, et obtenir un accès à des informations sensibles, dont les identifiants d'utilisateurs.

Par ailleurs, la faille CVE-2019-5591 est une vulnérabilité de la configuration par défaut dans FortiOS. Elle peut permettre à un attaquant distant et non authentifié d'intercepter des informations sensibles en se faisant passer pour le serveur LDAP.

Enfin, la vulnérabilité CVE-2020-12812 permet de contouner le processus d'authentification à deux facteurs dans le service VPN SSL de FortiOS. Elle est due à un défaut de traitement de la casse du nom d'utilisateur.

Correctifs et mises à jour

Les trois vulnérabilités sont connues de longue date, mais les correctifs que propose l'éditeur logiciel de Sunnyvale (Californie) ne sont pas forcément appliqués par les organisations.

Or, l'alerte du FBI et du CISA intervient à la suite de communications publiques multiples de Fortinet concernant la nécessité de mettre à niveau. Le fournisseur de solutions de sécurité réseau et terminaux l'a réaffirmé début avril 2021 dans un billet de blog.

« Appliquez les correctifs et les mises à jour de sécurité », exhortent les parties. En Europe, le CERT-FR a lui-même rappelé l'hiver dernier que « seule l'application de la mise à jour permet de [se] prémunir contre l'exploitation de la vulnérabilité correspondante ».

(crédit photo © Shutterstock)