Conflit ukrainien : les 19 failles que l'ANSSI conseille de patcher

« Cette faille que Fortinet traîne comme un boulet ». Ainsi titrions-nous, en septembre dernier, une actualité dont le fournisseur américain se serait volontiers passé. En l'occurrence, la fuite d'identifiants de connexion associés à près de 100 000 de ses passerelles VPN. Alors même que le correctif pour la vulnérabilité en question était disponible depuis plus de deux ans.

La faille se trouve dans le portail web de FortiOS. Elle permet, par traversement de répertoire, d'exfiltrer des données sur HTTP, sans authentification. L'ANSSI l'a incluse dans sa liste de vulnérabilités à colmater dans le contexte du conflit russo-ukrainien.

Cette liste comprend dix-huit autres failles, rendues publiques entre novembre 2017 et juillet 2021. Leur point commun : elles ont fait l'objet d'exploitations – ou de tentatives d'exploitation – par « des modes opératoires liés à la Russie ».

Exchange en tête des préoccupations de l'ANSSI

Six des failles listées affectent Microsoft Exchange. Parmi elles, il y a la CVE-2021-26855 (score CVSS : 9,8), principale de la série ProxyLogon. Elle permet de contourner l'authentification en envoyant, via Outlook Web Access, des requêtes HTTP arbitraires vers des ressources statiques. En combinaison avec d'autres vulnérabilités, elle a eu pour conséquence des vols d'e-mails et l'implantation de *webshells* sur des serveurs Exchange locaux.

Dans la lignée de ProxyLogon, il y eut ProxyShell. Les quatre failles de cette famille sont sur la liste de l'ANSSI : CVE-2021-33473 (9,8), CVE-2021-34523 (9,8), CVE-2021-31207 (7,2) et CVE-2021-31206 (8). Elles ont permis l'injection de code à distance au travers du port 443 ; en particulier grâce à une élévation de privilèges sur le *back-end* PowerShell.

La sixième faille (CVE-2020-0688 ; score de 8,8) peut occasionner une élévation de privilèges. Le problème se trouve au niveau de la création des clés uniques lors de l'installation.

Microsoft figure une septième fois dans la liste, avec une faille (CVE-2017-11882) qui touche Office. La source : une mauvaise gestion d'objets en mémoire. Le risque : une RCE (exécution de code à distance).

Deux des failles ont le score maximal (10). L'une (CVE-2019-7609) se trouve dans Kibana, au niveau du composant de visualisation Timelion. Elle pose un risque de RCE sans authentification. L'autre (CVE-2019-11510) touche plusieurs produits Pulse Secure. Elle peut permettre la lecture de fichiers arbitraires à distance.

Oracle figure deux fois sur la liste, avec les CVE-2019-2725 et CVE-2020-14082. Même score (9,8)… et même risque (RCE sans authentification).

Du risque de RCE, il y en a aussi avec les failles suivantes :

– Sur F5 BigIP, la CVE-2020-5902, au niveau de l'utilitaire de configuration (score : 9,8)

– La CVE-2019-19781 (9,8), présente dans plusieurs produits VMware

– Dans le composant mailboxd de Zimbra, une faille d'injection XML (CVE-2019-10149 ; score : 9,8)

– Sur Exim, la CVE-2019-10149 (9,8), liée à une mauvaise validation d'adresses de destinataires

OctoberCMS est aussi sur la liste, avec la CVE-2021-32648 (9,1), qui ouvre la porte à des réinitialisations indésirables de mots de passe… et ainsi à l'obtention d'accès à des comptes.

Toutes failles considérées, le score le plus bas (7,5) est à mettre à l'actif de la CVE-2019-1653. Elle touche plusieurs séries de routeurs Cisco. On a connaissance d'attaques qui ont permis d'obtenir des informations de configuration sensibles sans besoin de mot de passe.

Photo d'illustration © datacorpltd via *Visualhunt / CC BY-NC*