Exchange Server pris d'assaut : un SolarWinds bis ?

Quatre failles… pour des centaines de milliers de victimes. C'est sur ces chiffres que s'arrête le bilan provisoire d'une attaque révélée la semaine dernière. Sa cible : des serveurs Exchange locaux.

Il semble plutôt falloir parler de plusieurs attaques. Même si Microsoft s'attarde sur Hafnium, groupe cybercriminel dit à la solde de l'État chinois.

Les quatre failles fonctionnent en combinaison. L'une permet de contourner l'authentification en envoyant, *via* Outlook Web Access, des requêtes HTTP arbitraires vers des ressources statiques. Le chercheur qui l'a découverte lui a donné le nom de ProxyLogon.

> *The patch release of this BIG ONE is coming soon, and a short advisory is also standing by! (BTW, no one guess the right target in comments) https://t.co/EX1XgBxlkW*
>
> *— Orange Tsai (@orange_8361) March 2, 2021*

ProxyLogon permet d'accéder à des boîtes mail, parfois en connaissant simplement l'adresse des victimes. Elle ouvre la voie à l'exploitation des trois autres failles qui permettent d'exécuter du code à distance. Dans la pratique, elles ont entraîné l'injection de *webshells*.

Un SolarWinds version Exchange ?

Les correctifs – pour Exchange Server 2013, 2016 et 2019 – sont disponibles depuis mardi dernier. Depuis lors, les attaques semblent s'être intensifiées. Et avoir franchi un degré d'automatisation. On ne semble effectivement pas au même niveau de ciblage que dans l'affaire SolarWinds. Le nombre de victimes (30 000 estimées aux États-Unis) en témoigne. Sur place, la CISA, homologue de notre ANSSI, a publié une alerte et des directives. La Maison Blanche les a relayées.

Pour ceux qui ne peuvent appliquer immédiatement les correctifs, il existe des méthodes d'atténuation. Elles consistent, en fonction des failles, à mettre en place une règle IIS, à couper le service de messagerie unifiée ou encore à désactiver le pool d'applications OAB.

> *This is the real deal. If your organization runs an OWA server exposed to the internet, assume compromise between 02/26-03/03. Check for 8 character aspx files in C:\\inetpub\wwwroot\aspnet_client\system_web\. If you get a hit on that search, you're now in incident response mode. https://t.co/865Q8cc1Rm*
>
> *— Chris Krebs (@C_C_Krebs) March 5, 2021*

La première alerte est venue de Volexity. Les premières attaques que l'éditeur américain dit avoir identifiées remontent au 6 janvier. La veille, le chercheur ayant découvert ProxyLogon avait

communiqué ses trouvailles à Microsoft.

Illustration principale © Rawpixel.com – stock.adobe.com