Faille Citrix : gare aux effets secondaires

Les serveurs Citrix, des bombes à retardement ?

Des tiers semblent se réserver l'accès à certains d'entre eux en prévision de cyberattaques.

Leur porte d'entrée : la faille CVE-2019-19781, qui a secoué le monde de la sécurité IT ces dernières semaines.

Citrix en avait signalé l'existence le 17 décembre 2019. Et proposé par la même occasion des mesures d'atténuation – qui ne se sont pas révélées pleinement efficaces.

La mise à disposition de correctifs n'est intervenue qu'à partir du 20 janvier 2020, s'échelonnant jusqu'au 24. Entre-temps, les codes d'exploitation publics se sont multipliés.

Citrix ouvre les correctifs à tous les utilisateurs des produits affectés, qu'ils aient ou non un contrat de maintenance actif.

Toutes les versions de Citrix Gateway et Application Delivery Controller (anciennement exploités sous la marque NetScaler) sont touchées depuis la 10.5, dont la diffusion avait démarré en juin 2014. Les *appliances* SD-WAN le sont aussi, dans leur édition WANOP (WAN Optimization).

Attention, *backdoors*

Pour aider à la détection des machines infectées, Citrix propose un outil développé avec FireEye.

C'est de ce dernier que provient l'alerte relative aux cyberattaques « à retardement ».

Le principe : déployer, sur les serveurs vulnérables, une charge utile qui :

- supprime tout autre *malware* pour éviter d'attirer l'attention ;
- bloque les autres tentatives d'exploitation de la faille CVE-2019-19781 ;
- ouvre une *backdoor* accessible avec un mot de passe

Et FireEye d'inviter les entreprises à songer aux « effets secondaires » que pourrait impliquer une telle porte dérobée. L'installation de rançongiciels sur des postes Windows en est une.

> *Very tactical preliminary update. It appears an actor is using CVE-2019-19781 for initial access, and other vulnerabilities to pivot into a Windows environment in order to deploy ransomware. If you haven't already begun mitigating, you really need to consider the ramifications.*
>
> *— Andrew Thompson (@QW5kcmV3) January 23, 2020*

Chercheur pour la GDI Foundation, Victor Gevers scanne, trois fois par jour, les serveurs Citrix vulnérables. Le 31 décembre 2019, il en dénombrait près de 130 000. Il en resterait désormais un peu plus de 10 000.

Photo d'illustration © Citrix – CC BY-ND 2.0