Faille Windows 10 : la démarche inédite de la NSA

Patchez Windows 10, c'est la NSA qui le dit.

Pour la première fois, l'agence a accepté que Microsoft lui attribue la découverte d'une faille.

Ladite faille (CVE-2020-0601) touche aussi Windows Server 2016 et 2019.
Elle réside dans la CryptoAPI (Cryptographic Application Programming Interface).

Cette API permet d'utiliser les fonctions cryptographiques implémentées dans la bibliothèque CSP (Cryptographic Service Provider).
Parmi ces fonctions, il y a la vérification des signatures destinées à prouver l'authenticité de logiciels.

Problème : CryptoAPI n'applique pas les mesures de sécurité nécessaire pour valider certains certificats. En l'occurrence, ceux qui utilisent l'algorithme ECC (cryptographie sur les courbes elliptiques).

Le souci se pose uniquement sur les versions de Windows qui prennent en charge les clés ECC spécifiant des paramètres.

La NSA montre un visage plus collaboratif

Exploiter la faille peut permettre de faire passer tout certificat comme légitime. Et l'utiliser, entre autres, pour signer des exécutables malveillants.

Sont également touchées les applications qui utilisent la fonction CertGetCertificateChain() de Windows pour remonter les chaînes de certificats.

> *Love this, apropos of the Microsoft vulnerability much discussed today. https://t.co/Q1Oj5R7Lat*
>
> *— briankrebs (@briankrebs) January 14, 2020*

Aux organisations qui ne pourraient patcher tous leurs systèmes, la NSA recommande de prioriser :

- les serveurs et *appliances* web
- les proxys TLS
- les contrôleurs de domaines
- les serveurs DNS et VPN
- de manière plus générale, les terminaux exposés au réseau Internet

La présente démarche, affirme l'agence, s'inscrire dans le cadre d'une initiative « Turn a New Leaf » (« Tourner une nouvelle page »). Elle promet d'accentuer, dans ce cadre, sa communication avec les éditeurs de logiciels.

En toile de fond, l'exploit EternalBlue, que la NSA avait gardé au chaud… jusqu'à ce qu'il filtre et ouvre la voie à WannaCry.

Photo d'illustration © isak55 – Shutterstock.com