SolarWinds : plus de peur que de mal pour Microsoft ?

Microsoft a-t-il pris la pleine mesure de la campagne SolarWinds ? Le groupe américain s'estime en tout cas en capacité de livrer, à son périmètre, un bilan définitif. Principale conclusion : ni ses produits, ni ses systèmes internes n'ont servi de relais d'attaque.

Les accès indésirables à du code source se confirment, en revanche. Microsoft en avait fait état fin décembre. Il apporte désormais des précisions. D'une part sur la chronologie des événements (premier accès fin novembre ; tentatives jusqu'en janvier, mais la brèche était alors colmatée). De l'autre, sur les éléments concernés.

« Un petit nombre de dépôts », « seulement quelques fichiers »… À défaut d'une estimation précise du volume de code exposé, on retiendra les trois produits touchés : Exchange, Intune et Azure. Les journaux de requêtes indiquent une volonté de dénicher des secrets. Microsoft affirme qu'il n'était pas possible d'en trouver, en tout cas utilisables sur des systèmes en production.

Principale cible de la campagne SolarWinds, les États-Unis n'ont, eux, pas terminé leur enquête. Son dernier bilan recense 9 agences gouvernementales affectées et une centaines de victimes dans le secteur privé. Dont une bonne partie d'entreprises technologiques dont les produits « pourraient servir de support à d'autres intrusions ».

JetBrains fait partie des entreprises sur lesquelles des soupçons ont pesé. Cet éditeur n'est pas américain, mais tchèque. Les inquiétudes portaient sur son outil CI/CD TeamCity, qu'il dit utilisé par « plus de 300 000 » organisations. Elles semblent s'être éteintes.

Photo d'illustration © Aamon – Fotolia