Avast : porte ouverte au code malveillant ?

Avast vient de désactiver à distance l'une des composantes de son antivirus.

Cette décision fait suite à un avertissement signé de l'équipe Google Project Zero.

La composante en question est un interpréteur JavaScript. Elle fait partie du moteur d'analyse antivirus. Plusieurs indices suggèrent que son implémentation remonte à 2009.

> *Wow – Avast decided to disable their JavaScript interpreter globally!*
>
> *The vulnerability report they mention wasn't just me, it was a Project Zero collaboration with @natashenka* □□□
>
> *I think this is the right decision, it was a *lot* of attack surface. https://t.co/iFyry17HD0*
>
> *— Tavis Ormandy (@taviso) March 11, 2020*

Le moteur dépend du processus AvastSvc.exe, doté de hauts privilèges d'exécution… mais dépourvu d'un bac à sable. Ce qui facilite grandement l'exploitation des éventuelles failles qu'il abriterait.

Tavis Ormandy, membre de Project Zero, a extrait l'interpréteur et a publié un outil de recherche de vulnérabilités.
« Si vous [en] trouvez une […], elle est probablement critique », affirme-t-il.

Du côté d'Avast, on n'annonce pas d'échéance pour la mise à disposition d'un correctif. Tout au plus assure-t-on que la désactivation de l'interpréteur n'affectera pas le fonctionnement de l'antivirus.

> *2/2-The disablement of the emulator won't affect the functionality of our AV product, which is based on multiple security layers.*
>
> *— Avast (@avast_antivirus) March 11, 2020*

Photo d'illustration © Avast