Alerte partage ! Les antivirus ESET victimes d’une faille de sécurité. Mettez vite à jour le moteur d’analyse | Le Net Expert Informatique

Alerte partage ! Les antivirus ESET victimes d’une faille de sécurité. Mettez vite à jour le moteur d’analyse

Un chercheur du Project Zero de Google a dévoilé une vulnérabilité critique affectant plusieurs produits et logiciels proposés par l'éditeur de sécurité ESET. La vulnerabilité est exploitable à distance et permet l'exécution de code malveillant sur la machine visée.

Les solutions de sécurité, comme n'importe quel autre logiciel, sont également exposées à des failles de sécurité qui peuvent permettre à un attaquant d'exécuter du code sur la machine. C'est d'ailleurs probablement l'une des raisons ayant poussé la NSA et le GCHQ à orienter leurs efforts de reverse engineering sur les produits de Kaspersky et d'autres éditeurs antivirus, afin de transformer ces obstacles en porte d'entrée au système de la cible.
La faille décrite par le chercheur Tavis Ormandy, qui avait déjà décelé une vulnérabilité affectant les logiciels de Sophos en 2012, porte plus précisément sur le moteur d'émulation utilisé par les produits de la société ESET. Cet outil est utilisé par l'antivirus pour faire tourner les instructions exécutées par la machine dans un environnement isolé, afin de détecter du code potentiellement malveillant pour l'utilisateur.

Même la version Linux est touchée
Malheureusement, celui-ci présente une vulnérabilité permettant à l'attaquant d'exécuter du code en disposant d'un haut niveau de privilège. Outre cet aspect, l'attaque est envisageable via un certain nombre de vecteurs : web, messagerie, ou périphérique de stockage, tous étant susceptibles d'être scannés par les programmes d'ESET à la recherche de code malveillant. La faille affecte les logiciels même dans leur configuration par défaut.
La vulnérabilité affecte de nombreux logiciels proposés par ESET : NOD32 Antivirus pour Windows, Cyber Security Pro pour OS X, NOD32 pour Linux Desktop, Endpoint Security et NOD32 Business Edition.
Un correctif est également proposé par ESET depuis le 22 juin, afin de corriger la faille de sécurité repérée par le chercheur. Le blog post détaille notamment divers moyen d'exploiter la faille, ainsi que des mesures d'atténuations : ainsi, couper l'analyse temps réel des outils d'ESET pourrait réduire le risque, en désactivant l'analyse automatique dans les outils proposés par la société slovaque. Mais la meilleure solution reste évidemment de patcher. Et vite.

Source : http://www.zdnet.fr/actualites/les-antivirus-eset-victimes-d-une-faille-de-securite-39821472.htm
Par Louis Adam