Spectre : le rappel à l'ordre de Google

Spectre reste une menace bien réelle. Démo à l'appui, Google fait passer le message.

Le groupe américain s'était impliqué dans les travaux qui avaient mené à la révélation de cette classe de vulnérabilités. C'était début 2018. Depuis lors, les navigateurs web, cibles préférentielles, se sont renforcés. On y a intégré des mécanismes (isolation de sites, blocage de ressources d'origines multiples, etc.) destinés non pas à empêcher l'exploitation de Spectre, mais à minimiser les fuites de données qui pourraient en résulter.

Dans la pratique, ce n'est pas encore assez. Tout du moins d'après le PoC que Google vient de publier. Il vise V8, le moteur JavaScript de Chrome. Mais d'autres navigateurs sont concernés, nous affirme-t-on. La surface d'attaque va également au-delà de l'OS testé (Linux)… ainsi que du CPU (Core i7-6500U) : il est possible de mettre à mal jusqu'à la puce Arm Apple M1, « sans modification majeure » du PoC.

Spectre met à profit les effets secondaires de l'exécution spéculative sur les processeurs modernes. En l'occurrence, le fait que les résultats de ces exécutions en avance peuvent rester en cache. Chronométrer la différence entre les réussites et les échecs peut permettre d'ouvrir un canal d'extraction d'informations.

À raison de 1 ko/s de capacité d'exfiltration, le PoC que Google a publié n'est pas le plus performant de ceux qu'il a expérimentés. Mais sa mise en place est relativement simple. Et son exécution, assez rapide. Le tout sans requérir une horloge précise, moyennant l'exploitation d'une faiblesse dans le mécanisme de nettoyage du cache.

Illustration principale © LoKan Sardari via *Visualhunt / CC BY-NC-SA*