Un simple JavaScript fragilise la protection ASLR des puces

Les puces de plus grands fondeurs, Intel, AMD, ARM, AllWinner, Nvidia, sont vulnérables à une attaque via un code JavaScript capable de contourner la protection ASLR (Address space layout randomization) ou distribution aléatoire de l'espace d'adressage. Cette faille a été découverte par 5 chercheurs de l'Université de Vrije aux Pays-Bas.

L'attaque se nomme ASLR□Cache ou AnC et se focalise sur le MMU (memory management unit), l'unité de gestion de la mémoire. Il s'agit d'un composant peu connu, mais présent sur de nombreuses micro-architectures de puces. Il est en charge d'améliorer les performances des opérations de gestion de cache.

Les experts ont découvert que ce composant partage une partie de son cache avec des applications de moindre confiance comme les navigateurs. En conséquence, ils ont envoyé du code JavaScript malveillant ciblant spécifiquement ce partage de mémoire et la capacité à lire son contenu. « *Nous avons élaboré une attaque par canal auxiliaire et plus particulièrement une attaque du cache de type EVICT + TIME, capable de détecter les emplacements des pages dans la table des pages accessibles lors de la génération d'une table de pages par la MMU* », précisent les chercheurs. Ils ajoutent que « *sur l'architecture x86_64, notre attaque peut trouver des décalages au sein des 4 pages de tables accessibles via le MMU. Ce décalage au sein des pages réussit à casser 9 bits d'entropie, donc même l'implémentation complète d'ASLR en 36 bits d'entropie n'est pas sûre* ».

Un accès à des zones mémoire

Plus simplement, l'attaque AnC est capable de casser l'ASLR et permettre aux pirates de lire des portions de la mémoire de l'ordinateur. Ils peuvent ensuite se servir de ces tronçons de mémoire pour lancer des attaques plus complexes et gagner ainsi l'accès à l'ensemble du système d'exploitation. En effet, ASLR est un mécanisme de protection de la mémoire déployé sur les principaux OS. Il rend aléatoire l'emplacement où le code est exécuté dans la mémoire. En contournant ASLR, un attaquant sait quel code s'exécute et peut cibler cette zone mémoire pour voler ensuite des informations stockées dans la mémoire du PC.

Les chercheurs ont testé avec succès des attaques AnC via JavaScript sur Chrome et Firefox auprès de 22 micro-architectures de puces. Les expériences ont réussi même en présence de protections supplémentaires intégrées aux navigateurs comme des bloqueurs de JavaScript Timers. Pire encore, les spécialistes indiquent que les attaques AnC peuvent être utilisées pour relancer des campagnes sur le cache précédemment bloquées. Une porte ouverte à de vieux bugs que les fournisseurs pensaient avoir atténués. La seule façon de se protéger de cette menace est d'intégrer une extension comme NoScript au sein des navigateurs, empêchant ainsi le code JavaScript non approuvé de s'exécuter dans le butineur.

Les vulnérabilités, homologuées CVE, ont été rapportées aux différents constructeurs de puces, de navigateurs et d'OS. Une grande majorité, dont les fondeurs, a considéré que l'ASLR n'était peut-

être plus une protection suffisante et viable au moins pour les navigateurs.

A lire aussi :

Anatomie du malware super furtif, caché dans la mémoire des serveurs

Une backdoor cachée dans les derniers processeurs Intel ?

crédit photo : Intel