Des chercheurs développent une étonnante attaque web sur la DRAM | Le Net Expert Informatique

Des chercheurs développent une étonnante attaque web sur la DRAM

Des chercheurs ont réussi à exploiter un défaut nommé « Rowhammer » qui inquiéte depuis longtemps les experts de la sécurité informatique. Leur attaque, menée depuis le web, s'appuie sur JavaScript et cible la DRAM des ordinateurs, exposant des millions d'internautes.

On sait depuis plusieurs années que les cellules mémoire des ordinateurs sont vulnérables à une interférence intentionnelle. Mais un récent document de recherche explique comment mener une attaque depuis le web qui augmente considérablement le danger pour les utilisateurs. Ce document, publié par des institutions autrichiennes et françaises – il a été coécrit par Daniel Gruss et Stefan Mangard de l'Université de Technologie de Graz en Autriche, et par Clémentine Maurice de Technicolor et Eurecom en France – pourrait obliger les fondeurs à trouver en urgence une solution qui résout le défaut connu sous le nom de « Rowhammer ».
Pour augmenter la densité de la DRAM, les concepteurs n'ont cessé de rapprocher les cellules, les rendant vulnérables aux interférences électriques. Une technique décrite sous le nom de « rowhammering » permet de changer la valeur binaire des cellules adjacentes en activant de manière répétée une rangée donnée de cellules de mémoire. Pendant longtemps, les concepteurs se sont préoccupés de la fiabilité posée par cette fuite électrique, sans considérer la question de la sécurité. Mais cette approche est en train de changer rapidement.

Une attaque à distance en JavaScript
Plus tôt cette année, des chercheurs de Google ont annoncé qu'ils avaient réussi à développer deux exploits opérationnels : le premier leur a permis de mener une attaque par escalade de privilège et l'autre utilise le changement de polarité induit par le défaut « Rowhammer » pour obtenir des privilèges au niveau du noyau. Mais, pour que l'attaque réussisse, ils avaient été obligés d'installer leurs exploits sur la machine de l'utilisateur. Ce qui est remarquable dans ce nouveau document, c'est qu'une telle attaque pourrait être menée depuis le web en s'appuyant sur JavaScript. Le code proof-of-concept Rowhammer.js a été testé dans Firefox 39, « mais notre technique d'attaque est générique et peut être appliquée avec tout type d'architecture, de langage de programmation et d'environnement runtime », ont-ils écrit. Elle ne nécessite pas un accès physique à un ordinateur, ce qui la rend beaucoup plus dangereuse.
Cela signifie également qu'un grand nombre de personnes pourraient être ciblées depuis le web, ce qui augmente le pool de victimes potentielles. « Étant donné que l'attaque peut être lancée simultanément et furtivement contre un nombre arbitraire de machines, elle représente une énorme menace pour la sécurité », ont-ils ajouté. De plus, un grand nombre d'ordinateurs sont vulnérables, puisque l'attaque est indépendante du système d'exploitation, et que le bug « Rowhammer » affecte de nombreux types d'architectures de puces. Les chercheurs essayent encore de savoir combien de systèmes seraient vulnérables à leur attaque. Jusqu'à présent, ils n'ont pas développé d'exploit qui permettrait d'obtenir un accès root à un ordinateur en exploitant le « rowhammering », mais ils pensent que des pirates pourraient éventuellement étendre les capacités de l'exploit qu'ils ont découvert.

Bloquer JavaScript avec NoScript
Tant que les fondeurs ne trouvent pas de solution à long terme pour résoudre le problème Rowhammer.js, les chercheurs proposent d'inclure dans les navigateurs web un test permettant de vérifier si l'ordinateur est vulnérable. Si le test est positif, « JavaScript doit être mis sous contrôle pour éliminer la possibilité d'un exploit. Même si le système est très probablement résistant, il faut laisser à l'utilisateur la possibilité d'activer explicitement JavaScript quand il visite une page web », écrivent-ils. Une autre alternative serait de désactiver complètement JavaScript en utilisant une extension comme NoScript. Mais de nombreux sites web reposent sur JavaScript et sans lui, la consultation de ces sites devient problématique.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lemondeinformatique.fr/actualites/lire-des-chercheurs-developpent-une-etonnante-attaque-web-sur-la-dram-61920.html
Par Jean Elyan et IDG NS