Faille IMPORTANTE dans le noyau de Mac OS

Les experts en cyber-sécurité de Google ont rendu publique une faille de sécurité présente dans le noyau de MacOs. Cette vulnérabilité, considérée comme « très sévère », a d'abord été communiquée à Apple, qui ne l'a pas encore corrigée.

La découverte du hug a été effectuée par les chercheurs en sécurité informatique du Project Zéro, de Google. Le but de cette équipe est de traquer les vulnérabilités « zero-day », c'est-à-dire celles n'ayant pas encore fait l'objet d'une exploitation ou d'une correction.

Le noyau XNU au cœur du problème

Cette fois-ci, c'est le système d'exploitation d'Apple MacOs qui a été pointé du doigt par les experts de Google. Ou plus précisément son noyau hybride, XNU. Le problème vient du mécanisme de copie sur écriture, ou *copy-on-wrile* (COW). Celui-ci permet de créer des copies de ressources partagées par différents processus, afin d'optimiser la mémoire utilisée.

Mais ce procédé semble souffrir d'une implémentation imparfaite dans MacOs. Les experts de Project Zéro se sont en effet aperçus qu'il était possible de modifier une image système sans que le sous-système de gestion n'en soit informé. Cela signifie notamment qu'un individu malveillant pourrait en profiter pour corrompre un fichier, sans entraîner d'alerte.

Le délai de 90 jours écoulé

Conformément à sa politique, l'équipe Project Zéro a commencé par avertir Apple de cette vulnérabilité, en novembre dernier. Elle a alors laissé à la firme un délai de 90 jours pour résoudre le problème. Le laps de temps étant écoulé, elle a décidé de rendre publique la faille de sécurité, dans la catégorie « sévérité élevée », afin que les utilisateurs puissent prendre les mesures nécessaires.

Cependant, si Apple n'a pas encore corrigé la vulnérabilité, l'entreprise travaille avec les experts de Project Zéro pour y parvenir. Les deux entités ont entamé une collaboration, qui devrait aboutir prochainement à la publication d'un patch de sécurité.