Foxconn laisse des backdoor trainer dans des smartphones Android

Foxconn a-t-il introduit une backdoor dans les smartphones Android que l'industriel taïwanais fabrique ? L'expert en sécurité américain Jon Sawyer n'est pas loin de le penser. D'ailleurs, il l'affirme sans détour. *« Pork Explosion (nom qu'il donne à la vulnérabilité, NDLR) est une backdoor trouvée dans le système de démarrage (bootloader) des applications fournies par Foxconn*, indique le chercheur sur son blog. Elle *permet une attaque avec un accès physique à un terminal pour obtenir les droits d'accès, avec selinux (la barrière de sécurité Linux, NDLR) désactivé via USB. »*

Rappelons que Foxconn fabrique des smartphones pour de nombreuses marques dont certaines lui laissent le droit d'intégrer du code de bas niveau dans les appareils. Et notamment des bootloader. C'est notamment le cas (mais pas seulement) des terminaux M810 de InFocus et Robin de Nextbit, souligne l'expert. Sur ces terminaux, et d'autres, il est donc possible d'avoir accès aux contenus du smartphone sans authentification. Un véritable sésame pour la police et autres services d'enquête judiciaire, notamment.

Une erreur grossière de Foxconn

Aux yeux du chercheur, il s'agit d'une erreur grossière de Foxconn plus que d'une volonté de délivrer un accès caché aux terminaux pour les autorités. En fait, le code laissé par l'industriel permet un accès rapide aux terminaux pour des besoins de mise au point. C'est une méthode généralement prisée des constructeurs utilisée sur leurs prototypes pour faciliter les tests et débogages. Mais ces codes sont généralement retirés des terminaux destinés à la vente. *« Bien qu'il s'agisse évidemment d'une fonction de débogage, c'est une porte dérobée, quelque chose que nous devrions pas voir dans les appareils modernes, et un signe de grande négligence de la part de Foxconn »*, affirme Jon Sawyer. D'autant que l'exploitation de la backdoor est relativement simple, confirme-t-il.

Le chercheur a découvert cette vulnérabilité fin août. Il a immédiatement reporté sa découverte à Mike Chan, le directeur technique de Nextbit avant de se tourner vers les équipes de Google et Qualcomm en contact rapproché avec Foxconn. Mais à ce jour, aucune modification n'aurait été apportée par l'industriel, rapporte *Threat Post*. Nextbit a en revanche publié un correctif la veille de la publication de l'article de Jon Sawyer.

Lire également
Google corrige les failles logées dans les composants électroniques pour Android
QuadRooter, 4 vulnérabilités qui menacent des millions de smartphones Android
Une backdoor cachée dans les derniers processeurs Intel ?

Crédit photo : Jne Valokuvaus-Shutterstock