Google verse jusqu'à 30 000 dollars par faille découverte dans Android

Google accélère – enfin – sur la problématique de la sécurité du système d'exploitation mobile **Android**, avec une nouvelle initiative, les Android Security Rewards. L'objectif est de proposer des primes aux chercheurs en sécurité découvrant des vulnérabilités au sein d'Android.

Le montant de ces primes dépendra en grande partie de la qualité du rapport de bogue. Pour une faille critique, découvrir le bug rapporte 2000 dollars. Proposer un code de test permet de booster cette somme à 3000 dollars. Si le code de test prend la forme d'un composant CTS (Compatibility Test Suite), 1000 dollars de plus seront versés. Enfin, la fourniture d'un correctif compte pour 4000 dollars. Bref, **le couple CTS+Patch permet de toucher 8000 dollars**.

Les failles marquées comme étant d'un niveau élevé donnent droit à une prime allant de 1000 à 4000 dollars. Pour les vulnérabilités modérées, la somme sera comprise entre 500 et 2000 dollars. Enfin, pour les bugs peu importants, le maximum versé par Google sera de 1000 dollars.

Jusqu'à 30 000 dollars par faille !

Certaines failles permettront de toucher le jackpot. C'est ainsi le cas de celles permettant de **compromettre le kernel Linux** via une application ou un accès physique au terminal (10 000 dollars), voire à distance (20 000 dollars). La compromission des dispositifs de sécurité **TrustZone ou Verified Boot** rapportera 20 000 dollars (30 000 dollars si opérée à distance). Ne rêvez pas toutefois ; Android est particulièrement solide dans ce domaine.

Google est assez large concernant les failles acceptées. Elles pourront toucher le code du système et des applications proposés via le projet **AOSP** (Android Open Source Project), du code **OEM** (librairies et pilotes de périphériques), le noyau **Linux** et l'OS **TrustZone**. Côté terminaux physiques, les **Nexus 6 et 9** sont les deux seuls appareils retenus aujourd'hui. En plus des failles nécessitant un accès physique au terminal, celles touchant leur *firmware* seront prises en considération par Google.

Les applications **non-AOSP créées par Google** ne sont pas couvertes par ce programme. Toutefois, elles sont éligibles au Google Vulnerability Reward Program, avec des primes pouvant atteindre les 20.000 dollars. Les failles de la version Android du navigateur web **Google Chrome** seront prises en charge par le Chrome Reward Program, avec un montant maximal de 15.000 dollars, pour un exploit permettant de passer outre le bac à sable du butineur.

90 jours de discrétion

L'objectif des Android Security Rewards n'est pas seulement de détecter des failles de sécurité, mais aussi **de les corriger avant qu'elles ne fassent des dégâts**. Les chercheurs sont donc invités à patienter avant de divulguer les failles qu'ils ont découvertes, sous peine de ne rien recevoir de la part de Google.

Notez que la firme se met elle-même la pression, en ne forçant pas les développeurs à attendre qu'un correctif soit effectivement mis au point. Elle recommande toutefois de lui laisser un délai raisonnable pour corriger la faille, soit **un minimum de 90 jours**. Reste à savoir si ce délai sera suffisant pour les constructeurs et opérateurs, en général peu réactifs lorsqu'il s'agit de diffuser des correctifs de sécurité relatifs à Android.

À lire aussi :
600 millions de smartphones Samsung touchés par une faille critique
Google met à jour le moteur HTML d'Android, WebView
Android for Work : du BYOD à la sauce Google pour séduire les DSI
Google a supprimé la moitié des malwares sous Android en 2014
Project Zero : Google lâche du lest sur les failles Zero Day