DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Vulnerabilități critice care afectează dispozitive mobile cu sistem de operare Android

Descriere

La sfârșitul anului 2022 și începutul anului 2023, **Project Zero** a raportat optsprezece vulnerabilități 0-day în modem-urile Exynos produse de Samsung Semiconductor.

Din testele efectuate de Project Zero, cele mai grave patru vulnerabilități (CVE-2023-24033, CVE-2023-26496, CVE-2023-26497 și CVE-2023-26498) permit unui atacator să compromită de la distanță un telefon, fără nicio interacțiune cu utilizatorul, și necesită doar ca atacatorul să cunoască numărul de telefon al victimei. Cercetătorii sunt de părere că atacatori calificați ar putea crea rapid un *exploit* operațional pentru a compromite dispozitivele afectate.

Celelalte paisprezece vulnerabilități conexe (CVE-2023-26072, CVE-2023-26073, CVE-2023-26074, CVE-2023-26075, CVE-2023-26076 și alte nouă vulnerabilități cărora nu li s-au atribuit încă ID-uri CVE) nu sunt la fel de grave, deoarece acestea necesită posibilitatea ca un operator de rețea mobilă s[fie rău intenționat, fie ca un atacator să aibă cu acces local la dispozitiv.

Impact

Anunțurile Samsung Semiconductor oferă lista chipseturilor Exynos care sunt afectate de aceste vulnerabilități. Pe baza informațiilor de pe site-urile web publice, care cartografiază chipseturile cu dispozitivele, produsele afectate includ probabil:

- Dispozitive mobile de la Samsung, inclusiv cele din seriile S22, M33, M13, M12, A71, A53, A33, A21s, A13, A12 și A04;
- Dispozitive mobile de la Vivo, inclusiv cele din seriile S16, S15, S6, X70, X60 și X30;
- Dispozitivele din seriile Pixel 6 și Pixel 7 de la Google; și orice vehicule care utilizează chipset-ul Exynos Auto T5123.

Remediere

Este de așteptat ca termenele de aplicare a patch-urilor să varieze în funcție de producător. De exemplu, dispozitivele Pixel afectate au primit un patch de remediere pentru toate cele patru vulnerabilități în actualizarea de securitate din martie 2023.

Între timp, utilizatorii cu dispozitive afectate se pot proteja de vulnerabilități prin **dezactivarea apelurilor Wi-Fi** și a **apelurilor de voce prin LTE (VoLTE)** în setările dispozitivului, deși posibilitatea de a modifica această setare poate depinde de operatorul dvs. de telefonie.

Utilizatorii sunt încurajați să își **actualizeze dispozitivele cât mai curând posibil**, pentru a se asigura că rulează cele mai recente versiuni care rezolvă atât vulnerabilitățile de securitate dezvăluite, cât și cele nedezvăluite.

Alte patru vulnerabilități care nu au fost dezvăluite

În conformitate cu politica standard de dezvăluire Project Zero, cercetătorii publică informații despre vulnerabilitățile de securitate documentate la o anumită perioadă de timp după ce le raportează unui furnizor de software sau hardware. În unele cazuri rare, în care echipa a apreciat că atacatorii ar beneficia semnificativ mai mult decât cei care ar trebui să de protejeze de aceste vulnerabilități, dacă o vulnerabilitate ar fi dezvăluită, aceștia au făcut o excepție de la politică și au amânat divulgarea.

Datorită unei combinații foarte rare a nivelului de acces pe care îl oferă aceste vulnerabilități și a vitezei cu care ar putea fi creat un *exploit* operațional fiabil, Project Zero a decis să facă o excepție de politică pentru a amâna divulgarea celor patru vulnerabilități care permit executarea de cod de la distanță.

Sursa: https://googleprojectzero.blogspot.com/2023/03/multiple-internet-to-baseband-remote-rce.html