

غوغل تحذر من ثغرة أمنية في معظم هواتف أندرويد



أوضحت شركة غوغل أنها عثرت على دليل بشأن وجود ثغرة أمنية غير مصححة في نظام التشغيل أندرويد تستخدم في الهجمات، وتحمل (CVE-2019-2215) حاليا الاسم

وبالرغم من أن الثغرة الأمنية قد جرى إصلاحها في الإصدارات الأقدم من أندرويد، إلا أنها عاودت الظهور في الإصدارات الأحدث

وتوجد الثغرة الأمنية في نواة نظام التشغيل أندرويد، ويمكن استخدامها لمساعدة المهاجم في الحصول على وصول إلى المستخدم الجذر للجهاز.

ومن المفارقات أن الثغرة تم تصحيحها في ديسمبر/كانون الأول 2017 في إصدارات أندرويد 3.18 و 4.14 و 4.4 و 4.9، لكنها عثرت عليها في الإصدارات الأحدث من نظام أندرويد

• Google Pixel. • Google Pixel 1 XL. • ويعتقد باحثو غوغل أن الثغرة الأمنية تؤثر على نماذج هواتف أندرويد التالية العاملة بنسخة أندرويد 8.0 وما بعده
Google Pixel 2. • Google Pixel 2 XL • Huawei P20. • Xiaomi Redmi 5A. • Xiaomi Redmi Note 5. • Xiaomi A1. • Oppo A3. • Moto Z3. • Samsung Galaxy S7. • Samsung Galaxy S8. • Samsung Galaxy
هواتف شركة إل جي العاملة بنظام أندرويد أوريو S9.

وأوضح باحثو غوغل أن الاستغلال يتطلب تخصيصا ضئيلا أو معدوما لكل جهاز، مما يعني أنه يجب أن الاستغلال قادر على العمل عبر مجموعة واسعة من الهواتف، وذلك بالرغم من أنهم لم يؤكدوا ذلك من خلال المراجعات اليدوية، كما فعلوا للأجهزة المذكورة أعلاه

التابعة للشركة أن (TAG) الثغرة الأمنية، وأكدت في وقت لاحق مجموعة تحليل التهديدات Project Zero واكتشف فريق غوغل الأمني المسمى الثغرة مستخدمة في الهجمات

وهي شركة إسرائيلية معروفة NSO Group التابعة لغوغل: "نعتقد أن الثغرة الأمنية قد استغلت من قبل (TAG) وقالت مجموعة تحليل التهديدات "ببيعتها أدوات المراقبة والاستغلال

وكشف متحدث باسم مشروع أندرويد المفتوح المصدر أن هذه الثغرة لا يمكن استغلالها دون تدخل المستخدم، وهناك بعض الشروط التي يجب توفرها بها قبل أن يتمكن المهاجم من استغلال الثغرة الأمنية

وتابع المتحدث: "صنفت هذه المشكلة على أنها شديدة الخطورة بالنسبة لنظام أندرويد، وتتطلب تثبيت تطبيق ضار للاستغلال المحتمل، وأبلغنا شركاء أندرويد بها، وأصبح التصحيح متاحاً على النواة المشتركة لأندرويد

العاملة بأحدث نواة أندرويد، ليست معرضة للخطر (Google Pixel 3a) و (Google Pixel 3 XL) و (Google Pixel 3) وأضاف أن أجهزة

على تحديثات لهذه المشكلة كجزء من التحديث الأمني لشهر أكتوبر/تشرين (Google Pixel 2) و (Google Pixel) ومن المفترض أن تحصل أجهزة
الأول