"جوجل" تحذر من ثغرتين خطيرتين بنظام تشغيل أندرويد

السبت 13 سبتمبر 2025 08:00 م

سلطت جوجل الضوء على ثغرتين برمجيتين، هما CVE-2025-38352 وCVE-2025-48543، وتقول جوجل: "هناك مؤشرات على أن هذه الثغرات في نظام تشغيل أندرويد قد تكون مُستغلة بشكل محدود ومُستهدف".
وأوصت جوجل وفقا لما ذكره موقع "Phone arena"، إنه يجب التأكد من تثبيت آخر تحديث أمان أندرويد على هاتفك، حيث تؤثر ثغرة CVE-2025-38352 على نواة أندرويد، أو جوهر نظام تشغيل أندرويد، وتُحافظ النواة على سلاسة عمل كل شيء، وظهرت هذه الثغرة في جزء نظام أندرويد المسؤول عن المنبهات المُدمجة في التطبيقات، والتي تضمن تنفيذ مهام مُحددة في أوقات مُحددة.
كما ذُكر، أصلحت جوجل هذه المشكلة بتصحيح في تحديث أندرويد لشهر سبتمبر 2025 الذي صدر مؤخرًا، وللتأكد من تحديث هاتف أندرويد الخاص بك، انتقل إلى الإعدادات > حول الهاتف > إصدار أندرويد > تحديث أمان أندرويد.
إذا كان تاريخ التحديث 5 سبتمبر 2025 أو أحدث، فهذا يعني أن هذا الخلل قد تم تصحيحه على هاتفك، أما إذا لم يكن كذلك، فحدّث هاتفك فورًا.
أما الثغرة الثانية هي CVE-2025-48543، والتي تُظهر ثغرة خطيرة في Android Runtime (ART)، هذا هو الجزء من الهاتف الذي يُشغّل التطبيقات، والثغرة هي خطأ في معالجة الذاكرة، قد يُطوّر مُخترق تطبيقًا ضارًا يستغل هذه الثغرة الأمنية للحصول على صلاحيات أعلى من اللازم، نتيجةً لذلك، قد يتحكم التطبيق الضار بعمليات النظام التي عادةً ما تتحكم بها جوجل أو مُصنّع هاتفك فقط، ما يسمح له بالوصول إلى بياناتك الشخصية وبيانات اعتماد التطبيق، مثل كلمات المرور.
وتعتقد جوجل أن هذه العيوب قد استُغلّت، مع أن هذه الهجمات قد تقتصر على مستخدمي أندرويد المُستهدفين، مثل الصحفيين والعاملين الحكوميين والناشطين.

ولعل المثير للقلق هو أن جوجل تُشير إلى إمكانية استغلال CVE-2025-38352 وCVE-2025-48543 دون تدخل المستخدم، فبمجرد وصول البرنامج الخبيث إلى هاتفك، والذي غالبًا ما يكون تطبيقًا ضارًا، لن تحتاج إلى فعل أي شيء لإنجاح الهجوم.
ما عليك فعله الآن هو:
-تحديث هاتفك.
-تأكد من تثبيت أحدث إصدارات تحديثات الأمان على هاتفك.
-شغّل التطبيقات الموثوقة فقط، لا تُحمّل التطبيقات من متاجر تطبيقات خارجية.
-أبقِ Google Play Protect مُفعّلاً للمساعدة في اكتشاف التطبيقات الضارة قبل أن تُسبب لك مشاكل خطيرة.