أبل توسّع إصلاح ثغرة CoreGraphics المستغَلة CVE-2026-86950 ليشمل أجهزة iPhone وiPad الأقدم



وسّعت أبل إصلاح الثغرة CVE-2026-86950 في CoreGraphics، وهي عالية الخطورة واستُغلت في هجمات فعلية، لتشمل أجهزة أقدم، بعد أن صدرت تحديثات الأجهزة الأحدث الشهر الماضي.

- تحمل الثغرة المعرّف CVE-2026-86950 ودرجة CVSS تبلغ 8.8.
- هي كتابة خارج الحدود في CoreGraphics قد تتيح تنفيذ تعليمات برمجية عشوائية.
- يتطلب الاستغلال معالجة ملف مصمَّم بصورة خبيثة.
- استُغلت الثغرة في هجمات فعلية بحسب المصدر.
- الإصلاح يشمل الآن أجهزة iPhone وiPad الأقدم، بينما صدرت التحديثات الأولى الشهر الماضي.

أصدرت أبل إصلاحات لثغرة مستغَلة فعليًا لتشمل أجهزة iPhone وiPad الأقدم، في امتداد للحماية التي صدرت أولاً

لأجهزة أخرى الشهر الماضي.

ما الذي حدث

الثغرة المعرّفة بالرقم **CVE-2026-86950** (درجة CVSS: 8.8) هي كتابة خارج الحدود في CoreGraphics. وإذا عالج الجهاز ملفًا مصمَّمًا بصورة خبيثة فقد يتمكن المهاجم من تنفيذ تعليمات برمجية عشوائية. ويذكر المصدر أن الثغرة استُغلت في هجمات فعلية.

التحديث الأخير هو نقل للإصلاح نفسه إلى أجهزة أقدم لم تحصل عليه في الإصدار الأصلي.

لماذا يهم ذلك

تُبقي المؤسسات عادةً أجهزة iPhone وiPad القديمة في الخدمة، ومنها الأجهزة المشتركة والاحتياطية وأجهزة الموظفين الشخصية المستخدمة في العمل. وهذه أكثر الأجهزة عرضة لتفويت الدفعة الأولى من التحديثات. ولأن الاستغلال مؤكد، ويكفي لتحقيقه معالجة ملف، فإن الأجهزة غير المحدَّثة تمثل تعرضًا فعليًا.

لا يوضح المصدر هوية المهاجمين أو أهدافهم أو طرازات الأجهزة وإصدارات النظام المتأثرة تحديدًا، لذا ينبغي الرجوع إلى نشرة أبل الرسمية للاطلاع على القائمة الدقيقة.

النهج الموصى به

تعاملوا مع الأمر بوصفه مهمة تحديث ذات أولوية: حدّدوا الأجهزة المُدارة والشخصية المشمولة بتحديث الأجهزة الأقدم، وطبّقوا الإصلاح، وتحققوا من اكتماله عبر أدوات إدارة الأجهزة بدل الاعتماد على المستخدمين.

ما يجب فعله الآن

1. حصر جميع أجهزة iPhone وiPad، بما فيها الطرازات الأقدم والأجهزة المشتركة والشخصية التي تصل إلى بيانات المنشأة.
2. مراجعة نشرة أبل الرسمية الخاصة بـ CVE-2026-86950 لتأكيد الطرازات وإصدارات النظام التي يشملها الإصلاح.
3. دفع التحديث عبر نظام إدارة الأجهزة المحمولة ورصد الامتثال، وتصعيد الأجهزة التي لم تُحدَّث.
4. تقييد وصول الأجهزة التي لا يمكن تحديثها إلى البريد والأنظمة الحساسة أو عزلها.
5. تذكير الموظفين بتجنب فتح الملفات غير المتوقعة والإبلاغ عن المرفقات المشبوهة لفريق الأمن.