

ثغرة الكتابة خارج الحدود في CoreGraphics من Apple تؤثر على iOS و macOS و iPadOS



كشفت Apple عن ثغرة كتابة خارج الحدود في CoreGraphics تؤثر على iOS و macOS و iPadOS قد تتيح تنفيذ تعليمات برمجية عشوائية.

- الثغرة CVE-2026-86950 هي ثغرة كتابة خارج الحدود في مكون CoreGraphics من Apple
- تؤثر على iOS و macOS و iPadOS عبر منتجات Apple متعددة
- قد يؤدي الاستغلال الناجح إلى تنفيذ تعليمات برمجية عشوائية
- توصي CISA بتطبيق تدابير الحماية من المورد وتقييم الأصول المعرضة للإنترنت
- يجب على المؤسسات التوقف عن الاستخدام إذا لم تتوفر تدابير الحماية

نظرة عامة على الثغرة

كشفت Apple عن الثغرة **CVE-2026-86950**، وهي ثغرة كتابة خارج الحدود تؤثر على مكون CoreGraphics في iOS و macOS و iPadOS. يحدث هذا النوع من الثغرات عندما يكتب البرنامج بيانات خارج حدود مخازن الذاكرة المخصصة، مما قد يسمح للمهاجمين بتنفيذ تعليمات برمجية عشوائية على الأجهزة المتأثرة. تشكل هذه الثغرة خطراً كبيراً على المؤسسات التي تعتمد على أجهزة Apple في عملياتها التشغيلية.

المخاطر والتعرض

قد يؤدي الاستغلال الناجح لهذه الثغرة إلى تنفيذ تعليمات برمجية عشوائية، مما يمكّن المهاجمين من تشغيل تعليمات برمجية ضارة بصلاحيات التطبيق أو مكون النظام المتأثر. بالنسبة للمؤسسات الخاضعة للتنظيم في المملكة، يمثل هذا قلقاً خاصاً حيث تُستخدم أجهزة Apple للوصول إلى الأنظمة الحساسة أو بيانات العملاء أو البنية التحتية الحيوية. أصدرت وكالة الأمن السيبراني والبنية التحتية الأمريكية إرشادات توصي المؤسسات بتطبيق تدابير الحماية من المورد وتقييم تعرض كل أصل للإنترنت.

الاستجابة الموصى بها

يجب على المؤسسات إعطاء الأولوية لتطبيق التحديثات الأمنية وفقاً لتعليمات Apple. تؤكد إرشادات CISA على أهمية التصحيح القائم على المخاطر ومتطلبات الفرز الجنائي. في حال عدم توفر تدابير الحماية أو عدم إمكانية تطبيقها في الوقت المناسب، يجب على المؤسسات النظر في التوقف عن استخدام المنتجات المتأثرة حتى صدور التصحيحات. تتطلب عمليات نشر الخدمات السحابية اهتماماً خاصاً لضمان اتباع إرشادات التصحيح المعمول بها عبر جميع البيئات.

ما يجب فعله الآن

1. حصر جميع أجهزة iOS و macOS و iPadOS من Apple عبر المؤسسة والبيئات السحابية
2. تطبيق التحديثات الأمنية من Apple فوراً وفقاً لتعليمات المورد
3. تقييم تعرض كل أصل متأثر للإنترنت وتحديد أولويات التصحيح بناءً على المخاطر
4. مراجعة وتنفيذ متطلبات الفرز الجنائي للأنظمة المتأثرة
5. التوقف عن استخدام المنتجات المتأثرة حيث لا يمكن تطبيق تدابير الحماية في الوقت المناسب
6. توثيق أنشطة التصحيح والامتثال لإجراءات إدارة التغيير الداخلية