

ثغرة للحصول على صلاحيات الجذر في OpenBSD تستغل خلال عمره 37 عاماً في الذاكرة المشتركة



نشر باحثون أمنيون استغلالاً عملياً لرفع الصلاحيات المحلية في OpenBSD 7.9 يربط بين خلل قديم في تجاوز الأعداد الصحيحة بالذاكرة المشتركة وثغرة في النواة للحصول على صلاحيات الجذر.

- كشفت شركة Calif الأمنية عن استغلال لرفع الصلاحيات المحلية يؤثر على OpenBSD 7.9 ويحقق صلاحيات الجذر
- يربط الاستغلال بين خلل في تجاوز الأعداد الصحيحة عمره حوالي 37 عاماً في الذاكرة المشتركة وثغرة منفصلة في النواة
- يتجاوز الهجوم آلية KARL لعشوائية عناوين نواة OpenBSD والحمايات المادية SMEP و SMAP
- نشرت Calif تحليلاً تقنياً مفصلاً وكود إثبات المفهوم الكامل بعد إصدار OpenBSD للتحديثات
- تتطلب الثغرة وصولاً محلياً إلى النظام لاستغلالها

تفاصيل الاستغلال

كشفت شركة Calif الأمنية عن ثغرة رفع الصلاحيات المحلية تؤثر على OpenBSD 7.9 تتيح لمهاجم لديه وصول محلي للنظام الحصول على صلاحيات الجذر. يربط الاستغلال بين خللين منفصلين: خلل في تجاوز الأعداد الصحيحة في معالجة الذاكرة المشتركة يعود تاريخه إلى حوالي 37 عاماً، وثغرة منفصلة في النواة.

يُظهر الهجوم تجاوزاً لآليات أمنية متعددة مدمجة في OpenBSD، بما في ذلك **KARL** (الربط العشوائي لعناوين النواة) الذي يعشوي عناوين النواة عند الإقلاع، بالإضافة إلى الحماية المادية SMAP (منع الوصول في وضع المشرف) و SMEP (منع التنفيذ في وضع المشرف). صُممت هذه الحماية لمنع الوصول غير المصرح به للذاكرة وتنفيذ الأكواد بمستويات صلاحيات مرتفعة.

الإفصاح والتصحيحات

أبلغت Calif مشروع OpenBSD بالثغرات وفقاً لممارسات الإفصاح المسؤول. بعد إصدار OpenBSD تصحيحات تعالج كلا الخللين، نشرت الشركة الأمنية تحليلاً تقنياً مفصلاً مع كود إثبات المفهوم الكامل الذي يوضح سلسلة الاستغلال.

يؤكد نشر كود استغلال عملي على أهمية التصحيح الفوري، خاصة للمؤسسات التي تشغل OpenBSD في بيئات الإنتاج. رغم أن الثغرة تتطلب وصولاً محلياً للاستغلال—أي يجب أن يكون لدى المهاجم بالفعل مستوى معين من الوصول للنظام—إلا أنها تمثل مساراً مهماً لتصعيد الصلاحيات يمكن استغلاله بعد اختراق أولي بوسائل أخرى.

دلالات الأكواد القديمة

يبرز وجود خلل في تجاوز الأعداد الصحيحة عمره نحو أربعة عقود في أكواد الإنتاج التحديات المستمرة في تحديد ومعالجة الثغرات في قواعد الأكواد الناضجة، حتى في أنظمة التشغيل الموجهة للأمن مثل OpenBSD.

ما يجب فعله الآن

1. حصر جميع الأنظمة التي تشغل OpenBSD والتحقق من مستويات الإصدارات الحالية عبر بيانات الإنتاج والتطوير
2. تطبيق تصحيحات أمن OpenBSD المتاحة فوراً، مع إعطاء الأولوية للأنظمة المتصلة بالإنترنت والبنية التحتية الحرجة
3. مراجعة وتقييد صلاحيات الوصول المحلي على أنظمة OpenBSD لتقليل سطح الهجوم لرفع الصلاحيات
4. مراجعة سجلات النظام للكشف عن محاولات غير عادية لرفع الصلاحيات أو وصول غير متوقع بصلاحيات الجذر على منصات OpenBSD
5. تقييم ما إذا كانت أنظمة Unix القديمة في بيئتك قد تحتوي على ثغرات مماثلة طويلة الأمد في معالجة الذاكرة المشتركة
6. تحديث إجراءات إدارة الثغرات لتشمل المراجعة الدورية للنشرات الأمنية لجميع أنظمة التشغيل مفتوحة المصدر المستخدمة