

برمجية PEERSTITCH الخبيثة تستغل ثغرة في FortiOS لتنفيذ هجمات موجهة



جهات تهديد متقدمة تستغل ثغرة اجتياز المسار في نظام FortiOS من فور تينت لنشر برمجية PEERSTITCH الخبيثة المقيمة في الذاكرة والتي تتجاوز فحوصات الأمان على جلسات الشبكة الافتراضية الخاصة.

- الثغرة CVE-2025-61624 هي ثغرة اجتياز مسار في مفسر سطر الأوامر لأنظمة FortiOS و FortiPAM و FortiProxy و FortiSwitchManager بدرجة خطورة 5.4 على مقياس CVSS
- برمجية PEERSTITCH هي برمجية خبيثة من نوع ARM64 مقيمة في الذاكرة لم يتم الإبلاغ عنها سابقاً
- البرمجية الخبيثة تتجاوز فحوصات الأمان على جلسات الشبكة الافتراضية الخاصة الموسومة
- الهجمات منسوبة إلى جهات تهديد متقدمة مشتبه بها تستهدف البنية التحتية لفور تينت

تفاصيل الثغرة الأمنية

تم تحديد ثغرة اجتياز مسار تحمل الرمز **CVE-2025-61624** في مفسر سطر الأوامر لعدة منتجات من فورتينيت، بما في ذلك FortiOS و FortiPAM و FortiProxy و FortiSwitchManager. تحمل الثغرة درجة خطورة 5.4 على مقياس CVSS ويتم استغلالها بنشاط من قبل جهات تهديد متقدمة مشتبه بها لاختراق البنية التحتية لشبكات المؤسسات.

خصائص البرمجية الخبيثة PEERSTITCH

يستغل المهاجمون هذه الثغرة لنشر برمجية **PEERSTITCH** الخبيثة، وهي نسخة غير موثقة سابقاً مصممة لمعماريات ARM64. تعمل البرمجية الخبيثة كتهديد مقيم في الذاكرة، مما يجعل اكتشافها أكثر صعوبة من خلال أساليب الفحص التقليدية القائمة على الملفات. من القدرات الرئيسية لبرمجية PEERSTITCH قدرتها على تجاوز فحوصات الأمان على جلسات الشبكة الافتراضية الخاصة الموسومة، مما قد يسمح بالوصول غير المصرح به إلى قطاعات الشبكة المحمية.

التداعيات على المؤسسات السعودية

تواجه المؤسسات الخاضعة للتنظيم في المملكة والتي تشغل أجهزة الأمان من فورتينيت مخاطر متزايدة من حملة الاستغلال هذه. يعد استهداف البنية التحتية للشبكة الافتراضية الخاصة مثيراً للقلق بشكل خاص نظراً للاعتماد الواسع على طول الوصول عن بُعد عبر قطاعات الخدمات المالية والرعاية الصحية والبنية التحتية الحيوية. يجب على المؤسسات التعامل مع هذا الأمر كحدث تصحيح ذي أولوية وإجراء تحقق فوري من نشر منتجات فورتينيت لديها. تستلزم الطبيعة المقيمة في الذاكرة للبرمجية الخبيثة مراقبة معززة تتجاوز أساليب الكشف القياسية على نقاط النهاية.

ما يجب فعله الآن

1. إجراء جرد فوري لجميع أنظمة FortiOS و FortiPAM و FortiProxy و FortiSwitchManager من فورتينيت المنتشرة في المؤسسة
2. تطبيق التصحيحات الصادرة من المورد للثغرة CVE-2025-61624 على أساس الأولوية وفقاً لإجراءات إدارة التغيير
3. إجراء تحليل جنائي للذاكرة على جميع أجهزة فورتينيت للكشف عن إصابات محتملة ببرمجية PEERSTITCH
4. مراجعة سجلات جلسات الشبكة الافتراضية الخاصة للكشف عن نشاط جلسات موسومة شاذ ومحاولات وصول غير مصرح بها
5. تعزيز مراقبة نشاط مفسر سطر الأوامر في أنظمة فورتينيت وتطبيق قواعد الكشف السلوكي
6. التنسيق مع مزودي عمليات الأمان من الجهات الخارجية للتحقق من سلامة البنية التحتية المُدارة من فورتينيت