حملة تستهدف جدران الحماية وبوابات VPN وتكشف أكثر من 70 ألف بيانات اعتماد



كشف باحثون عن حملة واسعة تستهدف أجهزة الحافة المكشوفة، ومنها Fortinet FortiGate وPalo Alto Networks GlobalProtect، وتفيد النتائج بوصول المهاجمين إلى جهات كثيرة حول العالم ومحاولتهم التوسع داخل بعضها.

- تستهدف الحملة أجهزة الحافة الشبكية المكشوفة على الإنترنت.
- من المنتجات المذكورة جدارا الحماية Fortinet FortiGate وPalo Alto Networks GlobalProtect.
- يشير العنوان إلى كشف أكثر من 70 ألف بيانات اعتماد.
- تدل الأدلة المستخرجة من التحقيق على الوصول إلى جهات كثيرة حول العالم.
- حاول المشغّلون التوسع في اختراق بعض الضحايا.

ما الذي أُعلن

نشر باحثون تفاصيل حملة واسعة النطاق تستهدف أجهزة الحافة الشبكية التي يمكن الوصول إليها من الإنترنت. ومن المنتجات المذكورة في التقرير جدران الحماية Fortinet FortiGate وPalo Alto Networks GlobalProtect. ويشير عنوان التقرير إلى كشف أكثر من 70 ألف بيانات اعتماد.

ووفق الباحثين، تدل الأدلة المستخرجة من التحقيق على أن المشغّلين وصلوا إلى جهات كثيرة حول العالم، وحاولوا التوسع في اختراق بعض الضحايا.

أهمية الخبر

تقع جدران الحماية وبوابات VPN عند حدود الشبكة، وغالباً ما تتعامل مع بيانات اعتماد الوصول عن بُعد أو تحتفظ بها. وقد يمنح الوصول عند هذه الطبقة المهاجم نقطة انطلاق للتحرك داخل البيئة. ولا يوضح المقتطف المتاح التقنية المستخدمة أو أي ثغرات محددة أو القطاعات والدول المتأثرة، لذا ينبغي عدم افتراض سبب بعينه.

النهج المقترح

على الجهات التي تشغّل المنتجات المذكورة، أو أي بوابة وصول عن بُعد مكشوفة على الإنترنت، أن تعدّ الخبر دافعاً لمراجعة التعرّض وسلامة بيانات الاعتماد. والخطوات التالية احترازية ولا تتوقف على تأكيد ثغرة بعينها.

ما يجب فعله الآن

1. حصر جميع جدران الحماية وبوابات VPN المكشوفة على الإنترنت، ومنها أجهزة FortiGate وGlobalProtect.
2. إعادة تعيين بيانات الاعتماد المستخدمة في أجهزة الحافة وحسابات الوصول عن بُعد وفرض المصادقة متعددة العوامل.
3. مراجعة سجلات المصادقة والإدارة في أجهزة الحافة بحثاً عن تسجيلات دخول غير مألوفة أو تغييرات في الإعدادات.
4. التأكد من تشغيل أحدث إصدارات البرمجيات المدعومة من المورّد وحجب واجهات الإدارة عن الإنترنت العام.
5. فحص مؤشرات التحرك الجانبي من جلسات VPN ورفع أي نتائج عبر إجراءات الاستجابة للحوادث.