سيسكو تصدر تحديثات لثغرة يوم الصفر في ASA وFTD المستغلة لإيقاف جدران الحماية



أصدرت سيسكو تحديثات لثغرة يوم صفر تتيح حجب الخدمة في برمجيات ASA وThreat Defense (FTD)). ويستغلها مهاجمون فعلياً لإيقاف أجهزة جدران الحماية عن بُعد، ومنها خدمات SSL VPN.

- الثغرة من نوع حجب الخدمة (يوم صفر) في برمجيات Cisco ASA وFTD (Threat Defense).
- يستغلها مهاجمون فعلياً لإيقاف أجهزة جدران الحماية الضعيفة عن بُعد.
- أصدرت سيسكو تحديثات أمنية لمعالجة المشكلة.
- يشير عنوان الخبر إلى أن أجهزة SSL VPN ضمن الأجهزة المتأثرة بالتعطيل.
- المقتطف المتاح لا يتضمن رقم CVE أو قوائم الإصدارات المتأثرة، لذا يجب الرجوع إلى نشرة سيسكو.

أصدرت سيسكو تحديثات أمنية لثغرة يوم صفر في برمجيات Adaptive Security Appliance (ASA) وThreatg Defense (FTD). تتيح الثغرة حجب الخدمة، ويستغلها مهاجمون بالفعل لإيقاف أجهزة جدران الحماية الضعيفة عن بُعد.

ما المعروف حتى الآن

استُغلت الثغرة قبل توفر الإصلاح، ولذلك تُصنَّف يوم صفر. ووفق الخبر، يمكن دفع جدران الحماية المتأثرة إلى التعطل عن بُعد، ويشير العنوان تحديداً إلى تعطيل أجهزة SSL VPN. أما المقتطف المتاح لنا فلا يتضمن رقم CVE ولا الإصدارات المتأثرة ولا شروط الاستغلال التقنية.

لماذا يهم ذلك

تقع جدران الحماية وبوابات VPN على حافة الشبكة. وتكرار تعطلها قد يقطع الوصول عن بُعد للموظفين والشركاء، وقد يُضعف الحماية الطرفية إلى حين استعادة الجهاز. وبالنسبة للجهات المنظمة فهذه مسألة توافر واستمرارية أعمال بقدر ما هي مسألة أمنية.

النهج الموصى به

يُنصح بمعاملة الأمر كأولوية في التحديث لكل نشر لـ ASA أو FTD. تحققوا من التعرض عبر نشرة سيسكو الرسمية التي تبين الإصدارات المتأثرة والإصدارات المصححة، ونفّذوا التحديث وفق إجراء التغيير الطارئ المعتمد. وفي الأثناء، راقبوا أي إعادة تشغيل أو تعطل غير متوقع في أجهزة جدران الحماية، فقد يدل على محاولات استغلال.

ما يجب فعله الآن

1. حصر جميع أجهزة Cisco ASA وFTD، بما فيها التي تقدم SSL VPN، وتوثيق إصدارات برمجياتها.
2. مراجعة نشرة سيسكو الرسمية لمعرفة الإصدارات المتأثرة والمصححة وجدولة التحديث كتغيير طارئ.
3. مراقبة سجلات جدران الحماية وسلامة الأجهزة بحثاً عن تعطل أو إعادة تشغيل غير متوقعة والتحقيق فيها.
4. التأكد من فاعلية التبديل التلقائي أو التوافر العالي وترتيبات الوصول البديل عن بُعد عند تعطل بوابة.
5. الإبلاغ عن أي استغلال مؤكد أو انقطاع خدمة عبر إجراءات الحوادث، وإلى الجهة التنظيمية عند اللزوم.