SonicWall تحثّ عملاءها على استبدال جدران الحماية من الجيل السادس لتوقف التصحيحات الأمنية عنها



طلبت SonicWall من عملائها استبدال جدران الحماية من الجيل السادس فورًا وعدم تعريضها على حافة الإنترنت، إذ لن تتلقى تصحيحات أمنية حتى للثغرات الحرجة.

- تحثّ SonicWall جميع العملاء الذين يستخدمون جدران الحماية من الجيل السادس على إيقافها واستبدالها فورًا.
- تفيد الشركة بأن أجهزة Gen 6 لن تتلقى تصحيحات أمنية حتى للثغرات الحرجة.
- طُلب من العملاء عدم تعريض هذه الأجهزة على حافة الإنترنت.
- تشير الشركة إلى أن المهاجمين يستخدمون الأتمتة والذكاء الاصطناعي لاكتشاف الأجهزة غير المدعومة واستغلالها بسرعة أكبر.
- لا يذكر المصدر أرقام CVE محددة ولا حوادث مؤكدة.

وجّهت SonicWall تحذيرًا إلى العملاء الذين ما زالوا يشغّلون جدران الحماية من الجيل السادس (Gen 6)، مفاده ضرورة إيقاف هذه الأجهزة واستبدالها فورًا، وعدم إبقائها معرّضة على حافة الإنترنت.

ما تقوله الشركة

وفق ما ورد في التقرير، لن تتلقى أجهزة Gen 6 تصحيحات أمنية، بما في ذلك للثغرات الحرجة. وتبرر SonicWall ذلك بأن المهاجمين باتوا يستخدمون الأتمتة والذكاء الاصطناعي لاكتشاف أجهزة الحافة غير المدعومة واستغلالها أسرع من السابق، وتتوقع أن تكون جدران Gen 6 المواجهة للإنترنت هدفًا للهجمات.

لا يذكر المقتطف المتاح ثغرات بعينها ولا تواريخ ولا حالات اختراق مؤكدة، ولذلك ينبغي قراءة الخبر بوصفه تحذيرًا من الشركة بشأن انتهاء الدعم، وليس بلاغًا عن استغلال محدد.

الأهمية للجهات المنظَّمة

يمثّل جدار الحماية الطرفي الذي لا يمكن تحديثه تعرّضًا دائمًا؛ فأي ثغرة تُكتشف مستقبلاً ستبقى مفتوحة في جهاز يقع عند الحد الفاصل بين الشبكة الداخلية والإنترنت. وبالنسبة للجهات الخاضعة لمتطلبات الهيئة الوطنية للأمن السيبراني والبنك المركزي السعودي، يصعب تبرير تشغيل تقنية غير مدعومة على الحافة في تقييمات المخاطر وعمليات التدقيق.

والاستجابة العملية هي التحقق سريعًا من وجود أي أجهزة Gen 6 قيد التشغيل، بما في ذلك الفروع والمواقع البعيدة ولدى مشغّلين من أطراف ثالثة، ثم وضع خطة استبدال بأولويات واضحة بحسب درجة التعرّض.

ما يجب فعله الآن

1. حصر جميع جدران SonicWall وتحديد أي أجهزة من الجيل السادس، بما فيها أجهزة الفروع وتلك التي يديرها أطراف ثالثة.
2. إزالة أجهزة Gen 6 من التعرّض المباشر للإنترنت في أقرب وقت، أو تقييد الوصول إليها ريثما يتم الاستبدال.
3. وضع خطة استبدال بأولويات، تبدأ بالأجهزة الواقعة على حافة الإنترنت.
4. تسجيل الأجهزة غير المدعومة في سجل المخاطر مع تحديد المسؤول والضوابط المؤقتة وتاريخ مستهدف للإيقاف.
5. تعزيز مراقبة السجلات ومحاولات الوصول على أي جدار Gen 6 يتعذر إيقافه مؤقتًا.