# سونيك وول تصدر تصحيحات لثغرة بدرجة CVSS 10.0 قبل المصادقة في أجهزة SMA1000




أصدرت SonicWall تصحيحات عاجلة لأربع ثغرات في أجهزة الوصول عن بعد SMA1000، أخطرها بدرجة CVSS 10.0 تتيح لمهاجم دون تسجيل دخول تمرير طلبات عبر الجهاز إلى وظائف داخلية.

- أصدرت SonicWall تصحيحات عاجلة لأربع ثغرات في أجهزة SMA1000.
- توفر هذه الأجهزة للموظفين عن بعد منفذاً إلى شبكة الشركة وتطبيقاتها.
- أخطر الثغرات مصنفة 10.0 على مقياس CVSS.
- يستطيع المهاجم دون تسجيل دخول تمرير طلبات عبر الجهاز والوصول إلى وظائف داخلية.
- تفيد الشركة بعدم وجود دليل على استغلال أي من الثغرات الأربع.

نشرت SonicWall تصحيحات عاجلة لأربع ثغرات تؤثر في أجهزة SMA1000، وهي البوابات التي تعتمد عليها

المؤسسات لتمكين الموظفين عن بعد من الوصول إلى الشبكة الداخلية والتطبيقات.

## ما الذي أُعلن

تبلغ درجة أخطر الثغرات 10.0 على مقياس CVSS، وهي الدرجة القصوى. وبحسب التقرير، يمكن لمهاجم لا يملك بيانات دخول استغلالها لتمرير طلبات عبر الجهاز والوصول إلى وظائف داخلية. ولا يفصّل المصدر الثغرات الثلاث الأخرى.

وتذكر SonicWall أنه لا يوجد لديها دليل على استغلال أي من الثغرات الأربع. وهذا مطمئن، لكنه لا يبرر التأخير، فالثغرات التي لا تتطلب مصادقة على بوابة متاحة عبر الإنترنت تلفت انتباه المهاجمين بمجرد صدور الإصلاح.

## الخطوات المقترحة

على الجهات التي تشغّل SMA1000 تحديد الأجهزة المتأثرة، وتطبيق التصحيحات عبر مسار التغيير الطارئ المعتمد، ومراجعة سجلات الجهاز الأخيرة بحثاً عن طلبات غير معتادة. ويُعامل ذلك كمعالجة ذات أولوية لبنية الوصول عن بعد المكشوفة خارجياً، مع توثيق القرار وتاريخ الإنجاز لأغراض التدقيق.

## ما يجب فعله الآن

1. حصر جميع أجهزة SMA1000 لديكم ومطابقتها مع نشرة SonicWall.
2. تطبيق التصحيحات الصادرة عبر مسار تغيير مستعجل.
3. مراجعة سجلات الجهاز والمحيط الشبكي بحثاً عن طلبات داخلية غير معتادة.
4. تقييد واجهات الإدارة وحصر تعرّض الجهاز على الحد الضروري.
5. توثيق المعالجة وتاريخ إنجازها كدليل للتدقيق وفق ضوابط ECC وإطار SAMA CSF.