SonicWall publicó una advertencia sobre tres vulnerabilidades en sus dispositivos Secure Mobile Access (SMA) 1000, incluyendo una vulnerabilidad de omisión de autenticación de alta gravedad.

Las vulnerabilidades afectan a SMA 6200, 6210, 7200, 8000v, con versiones de firmware 12.4.0 y 12.4.1. Las vulnerabilidades son:

- CVE-2022-22282 (puntaje CVSS: 8.2) – Omisión de control de acceso no autenticado
- CVE-2022-1702 (puntaje CVSS: 6.1) – Redirección de URL a un sitio no confiable (redireccionamiento abierto)
- CVE-2022-1701 (puntaje CVSS: 5.7) – Uso de una clave criptográfica compartida y codificada

La explotación exitosa de los errores mencionados podría permitir a un atacante acceder sin autorización a los recursos internos e incluso redirigir a las posibles víctimas a sitios web maliciosos.

A Tom Wyatt, del equipo de seguridad ofensiva de Mimecast, se le atribuye el descubrimiento y el informe de las vulnerabilidades.

SonicWall dijo que las vulnerabilidades no afectan a la serie SMA 1000 que ejecuta versiones anteriores a la 12.4.0, la serie SMA 100, los servidores de administración central (CMS) y los clientes de acceso remoto.

Aunque aún no hay evidencia de que estas vulnerabilidades estén siendo explotadas en la naturaleza, se recomienda que los usuarios apliquen las correcciones sabiendo que los dispositivos SonicWall han presentado atracción para los ataques de ransomware.

> *«No hay mitigaciones temporales. SonicWall insta a los clientes afectados a implementar los parches correspondientes lo antes posible»,* dijo la compañía.