SonicWall reveló este miércoles que una parte no autorizada accedió a los archivos de respaldo de configuración de cortafuegos (firewall) pertenecientes a todos los clientes que han utilizado su servicio de copias de seguridad en la nube.

"Los archivos contienen credenciales cifradas e información de configuración; aunque el cifrado permanece activo, el hecho de que alguien tenga estos archivos podría aumentar el riesgo de ataques dirigidos", indicó la empresa.

También señaló que está en proceso de notificar a todos sus socios y clientes, y que ha puesto a disposición herramientas que permiten evaluar los dispositivos y aplicar medidas correctivas. Además, instó a los usuarios a iniciar sesión en su cuenta para revisar el estado de sus dispositivos registrados.

Esta situación se presenta semanas después de que SonicWall pidiera a sus usuarios restablecer sus credenciales tras haberse detectado una brecha de seguridad que expuso archivos de respaldo de configuración en cuentas de MySonicWall.

La lista de dispositivos comprometidos disponible en el portal MySonicWall ha sido clasificada por niveles de prioridad, con el fin de facilitar a los usuarios la organización de sus acciones de mitigación. Las categorías asignadas son las siguientes:

- Activo – Alta Prioridad: Dispositivos con servicios accesibles desde internet habilitados
- Activo – Baja Prioridad: Dispositivos sin servicios expuestos a internet
- Inactivo: Equipos que no se han conectado al sistema durante los últimos 90 días

El análisis más reciente representa un cambio con respecto a la evaluación inicial, en la que la empresa aseguraba que los archivos de preferencias de firewall almacenados en la nube habían sido accedidos solo en menos del 5% de los casos. También se indicó en ese momento que, aunque las credenciales estaban cifradas, los archivos incluían *"información que podría facilitar a los atacantes la explotación del firewall correspondiente"*.

Actualmente no se ha revelado cuántos clientes usan el sistema de respaldo en la nube, ni

cuándo comenzaron los ataques o quién estaría detrás. Sin embargo, SonicWall aseguró que ha reforzado su infraestructura, implementado una mayor capacidad de registro y aplicado controles de autenticación más estrictos para evitar incidentes similares.

Se recomienda a los usuarios seguir los siguientes pasos de inmediato:

1. Iniciar sesión en su cuenta de MySonicWall.com y verificar si existen respaldos en la nube para los firewalls registrados.
2. Si los campos están vacíos, no hay indicios de impacto.
3. Si aparecen detalles de respaldo, verificar si los números de serie afectados figuran en la cuenta.
4. Si se muestran los números de serie, deben seguirse las pautas de contención y corrección correspondientes a esos dispositivos.

SonicWall añadió que, en los casos donde se haya utilizado la función de respaldo en la nube pero no aparezcan números de serie —o solo se muestre una parte de ellos—, se proporcionarán instrucciones adicionales en los próximos días.