SonicWall advirtió a sus usuarios este lunes sobre intentos de explotación activos de una vulnerabilidad de día cero en sus dispositivos de la serie Secure Mobile Access (SMA) 100.

La vulnerabilidad, que afecta tanto a dispositivos SMA 100 10.x físicos como virtuales (SMA 200, SMA 210, SMA 400, SMA 410, SMA 500v), salió a la luz luego de que el Grupo NCC alertó el domingo que había detectado *«el uso indiscriminado de un exploit en la naturaleza».*

Los detalles del exploit no se han revelado para evitar que el 0-day se explote aún más, pero se espera que un parche esté disponible a este 2 de febrero de 2021.

> *«Algunos miles de dispositivos se ven afectados. El firmware SMA 100 anterior a 10.x no se ve afectado por esta vulnerabilidad de día cero»*, dijo SonicWall.

El 22 de enero, The Hacker News reveló que SonicWall había sido violado como consecuencia de un ataque cibernético coordinado en sus sistemas internos mediante la explotación de *«probables vulnerabilidades de día cero»* en sus dispositivos de acceso remoto de la serie SMA 100.

Después, el 29 de enero, la compañía emitió una actualización indicando que hasta ahora solo había observado el uso de credenciales previamente robadas para iniciar sesión en los dispositivos de la serie SMA 100.

Aunque SonicWall no ha compartido muchos detalles sobre la intrusión citando la investigación en curso, el último desarrollo apunta a la evidencia de que un zero day crítico en el código 10.x de la serie SMA 100 puede haber sido explotado para llevar a cabo el ataque.

Mientras tanto, SonicWall rastrea internamente la vulnerabilidad como SNWLID-2021-0001.

La compañía dijo que los firewalls SonicWall y los dispositivos de la serie SMA 100, así como todos los clientes VPN respectivos, no se ven afectados y siguen siendo seguros de usar.

La compañía está recomendando a sus clientes que habiliten la autenticación multifactor (MFA) y restablezcan las contraseñas de usuario para las cuentas que utilizan la serie SMA 100 con firmware 10.x.

«Si la serie SMA 100 (10.x) está detrás de un firewall, bloquee todo el acceso al SMA 100 en el firewall», dijo la compañía. Los usuarios también cuentan con la opción de apagar los dispositivos vulnerables de la serie SMA 100 hasta que haya un parche disponible o cargar la versión de firmware 9.x después de reiniciar la configuración predeterminada de fábrica.

Actualización 3 de febrero de 2021

SonicWall compartió con Masterhacks su actualización de firmware para parchear la vulnerabilidad Zero-Day en el código 10.x de la serie SMA 100.

> *«Todos los clientes de SonicWall con dispositivos activos de la serie SMA 100 que ejecutan código 10.x deben aplicar inmediatamente el parche en dispositivos físicos y virtuales. El parche también contiene código adicional para fortalecer el dispositivo.»,* dice el comunicado de SonicWall.

Para poder actualizar el firmware, los usuarios deben leer el artículo KB, ya que en él se describe cómo actualizar a la última versión a través de MySonicWal.

Los dispositivos de la serie 100 requieren el parche:

- Dispositivos físicos: SMA 200, SMA 210, SMA 400, SMA 410
- Dispositivos virtuales: SMA 500v (Azure, AWS, ESXi, HyperV)

> *«Como se indicó anteriormente, los firewalls SonicWall y los dispositivos de la serie SMA 1000, así como todos los respectivos clientes VPN, no se ven afectados y siguen siendo seguros de usar. Ninguna acción para estos productos es necesaria»,*

> agregó SonicWall.