BOLETÍN DE ALERTA

Boletín Nro.: 2023-08
Fecha de publicación: 13/03/2023
Tema: Nuevo *malware* afecta dispositivos SonicWall

Software afectado:

- SonicWall Secure Mobile Access (*SMA*).

Descripción:

Una supuesta campaña china de ciberataques se ha centrado en los dispositivos SonicWall Secure Mobile Access (SMA) sin parches para instalar malware personalizado que establece la persistencia a largo plazo para las campañas de ciber espionaje.

Este nuevo *malware* que es persistente a las actualizaciones de *firmware* en dispositivos SonicWall. El malware se compone de un binario *ELF*, una puerta trasera *TinyShell* y varios scripts bash, permitiendo a los atacantes ejecutar comandos *SQL* para lograr el robo de credenciales codificadas de todos los usuarios que iniciaron sesión.

Las credenciales robadas se copian en un archivo de texto creado por el atacante en *tmp/ syslog.db* y luego se recuperan para descifrarlas sin conexión. Además, el malware ejecuta otros componentes como *TinyShell*, de manera a obtener una *shell* reversa en el dispositivo para facilitar el acceso remoto.

Componentes del *malware*

Path	Hash	Function
/bin/firewalld	e4117b17e3d14fe64f45750be71dbaa6	Main malware process
/bin/httpsd	2d57bcb8351cf2b57c4fd2d1bb8f862e	TinyShell backdoor
/etc/rc.d/rc.local	559b9ae2a578e1258e80c45a5794c071	Boot persistence for firewalld
/bin/iptabled	8dbf1effa7bc94fc0b9b4ce83dfce2e6	Redundant main malware process
/bin/geoBotnetd	619769d3d40a3c28ec83832ca521f521	Firmware backdoor script
/bin/ifconfig6	fa1bf2e427b2defffd573854c35d4919	Graceful shutdown script

Fuente: https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/sonicwall-devices-infected-by-malware-that-survives-firmware-upgrades/amp/

Impacto:

La explotación exitosa de este *malware* permitiría a un atacante obtener credenciales de accesos de los usuarios y acceder a los dispositivos afectados a través de una consola de comandos *shell*.

Prevención:

Se recomienda a los administradores del sistema que apliquen las actualizaciones de seguridad más recientes (versión 10.2.1.7 o superior) proporcionadas por SonicWall que incluye Monitoreo de Integridad de Archivos (*FIM, por sus siglas en inglés*) e identificación de procesos anómalos que debería detectar y detener esta amenaza, en dispositivos SonicWall Secure Mobile Access (SMA).

Para información sobre la actualización de SMA 100 series a 10.2.1.7 puede consultar los siguientes enlaces:

- https://www.sonicwall.com/support/product-notification/sma-100-series-openssl-library-update-in-10-2-1-7/230228123000903/
- https://blog.sonicwall.com/en-us/2023/03/new-sma-release-updates-openssl-library-includes-key-security-features/

Para obtener más información sobre como actualizar el firmware de SonicWall puede consultar el siguiente enlace:

- https://www.sonicwall.com/support/knowledge-base/how-can-i-upgrade-sonicos-firmware/170504337655458/

Información adicional:

- https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/sonicwall-devices-infected-by-malware-that-survives-firmware-upgrades/amp/
- https://www.thehindu.com/sci-tech/technology/sonicwall-devices-infected-with-persistent-malware-by-suspected-chinese-hacking-campaign-report/article66602897.ece
- https://www.mandiant.com/resources/blog/suspected-chinese-persist-sonicwall
- https://www.sonicwall.com/products/remote-access/vpn-clients/
- https://www.sonicwall.com/support/product-notification/sma-100-series-openssl-library-update-in-10-2-1-7/230228123000903/