BOLETÍN DE ALERTA

Boletín Nro.: 2021-35

Fecha de publicación: 10/12/2021

Tema: Múltiples vulnerabilidades detectadas en productos SonicWall.

Dispositivos afectados:

- SMA 100 Series: SMA 200, 210, 400, 410, 500v (ESX, Hyper-V, KVM, AWS, Azure)

Descripción:

Se han identificado un total de ocho fallos de seguridad que afectan a los productos Secure Mobile Access (SMA) 100 de SonicWall.

A continuación, se describen las vulnerabilidades:

CVE-2021-20038 de severidad critica con una puntuación de 9.8, esta vulnerabilidad se debe al método GET del servidor *httpd Apache SonicWall SMA SSLVPN* en las variables de entorno del módulo *mod_cgi* que utilizan un único búfer en la pila utilizando "*strcat*". Esto podría permitir que un atacante remoto no autenticado realice ejecución del código como el usuario *nobody* en el dispositivo vulnerable.

CVE-2021-20039 de severidad alta con una puntuación de 7.2, esta vulnerabilidad se debe al método *http POST HTTP "/cgi-bin/viewcert" de SonicWall SMA SSLVPN* que permite a los usuarios autenticados cargar, ver o eliminar certificados SSL. Un atacante autenticado de forma remota puede ejecutar comandos arbitrarios utilizando este método http POST.

CVE-2021-20040 de severidad media con una puntuación de 6.5, esta vulnerabilidad se debe a la vulnerabilidad de ataque *path traversal*. Esta vulnerabilidad comparte la funcionalidad que permite a un atacante remoto no autenticado cargar archivos arbitrarios en cualquier directorio del dispositivo. Un atacante podría cargar páginas web creadas al directorio raíz del servidor web o archivos maliciosos en cualquier directorio del dispositivo como un usuario "*nobody"* en el dispositivo vulnerable.

CVE-2021-20041 de severidad alta con una puntuación de 7.5, esta vulnerabilidad se debe a la sobrecarga de la CPU debido a las solicitudes HTTP creadas y enviadas a https://address/fileshare/sonicfiles/sonicfiles provocando un bucle infinito en el proceso "*fileexplorer"*. Esto permitiría consumir todos los recursos de la CPU del dispositivo, causando una denegación de servicio, a un atacante no autenticado.

CVE-2021-20042 de severidad media con una puntuación de 6.3, la explotación de esta vulnerabilidad podría permitir que un atacante remoto no autenticado utilice el dispositivo como un "proxy" permitiéndose evadir filtros de *firewalls*.

CVE-2021-20043 de severidad alta con una puntuación de 8.8, esta vulnerabilidad se debe

al método *RAC_GET_BOOKMARKS_HTML5* que permite a los usuarios enumerar sus marcadores. Este método es vulnerable al desbordamiento de búfer debido al uso no verificado de *strcat*. Un atacante autenticado remotamente podría realizar ejecución de código como usuario "*nobody"* en el dispositivo vulnerable.

CVE-2021-20044 de severidad alta con una puntuación de 7.2, esta vulnerabilidad se debe a una API de administración expuesta que está escrita en *Python Flask*. Un atacante autenticado de forma remota podría ejecutar comandos del sistema como usuario "*nobody*" en el dispositivo vulnerable. El atacante podría modificar y/o eliminar archivos en el directorio *cgi-bin* y también podría reiniciar el dispositivo de forma remota.

CVE-2021-20045 de severidad critica con una puntuación de 9.4, esta vulnerabilidad se debe al método *RAC_COPY_TO* que permite a los usuarios cargar archivos en un recurso compartido *SMB* sin autenticación. *RAC_COPY_TO* se asigna al método *upload_file* de *Python* el cual está asociado con el binario *filexplorer* permitiendo a un atacante ejecutar comando de forma remota sin estar autenticado.

Los dispositivos de la serie SMA 100 con WAF habilitado también se ven afectados por la mayoría de estas vulnerabilidades.

Impacto:

La explotación de estas vulnerabilidades permitiría a un atacante comprometer la integridad de los datos, así como ejecutar código malicioso en el sistema en que se encuentra instalada la aplicación.

Solución:

Se recomienda actualizar a la versión más reciente del firmware instalado en el dispositivo, para más información ingresar en la siguiente URL:

- Product Security Notice: SMA 100 Series Vulnerability Patches (Q4 2021) | SonicWall

Información adicional:

- https://nvd.nist.gov/vuln/detail/CVE-2021-20038
- https://nvd.nist.gov/vuln/detail/CVE-2021-20039
- https://nvd.nist.gov/vuln/detail/CVE-2021-20040
- https://nvd.nist.gov/vuln/detail/CVE-2021-20041
- https://nvd.nist.gov/vuln/detail/CVE-2021-20042
- https://nvd.nist.gov/vuln/detail/CVE-2021-20043
- https://nvd.nist.gov/vuln/detail/CVE-2021-20044
- https://nvd.nist.gov/vuln/detail/CVE-2021-20045
- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026