Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°165	Fecha: 13-07-2023
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Nuevas vulnerabilidades reveladas en los productos de seguridad de red de SonicWall y Fortinet		
Tipo de Ataque	Intento de acceso con vulneración de credenciales	Abreviatura	IAVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

El 12 de julio 2023, la compañía Sonic Wall recomendó a sus clientes del software de gestión de firewall y motor de informes de red Analytics "Global Management System" (GMS), utilizar las ultimas correcciones para resguardarse contra 15 fallas de seguridad que pueden ser explotadas por un actor de amenazas para esquivar la autenticación y acceder a información confidencial.

De las 15 deficiencias (seguidas desde CVE-2023-34123 hasta CVE-2023-34137), cuatro tienen una calificación crítica, cuatro tienen una calificación alta y siete tienen una calificación de gravedad media.
Las vulnerabilidades fueron reveladas por NCC Group.

La compañía Fortinet también descubrió una falla crítica que afecta a FortiOS y FortiProxy (CVE-2023-33308, puntaje CVSS: 9.8) que podría facultar que un adversario obtenga la ejecución remota de código bajo ciertas circunstancias. Cabe indicar que el problema se resolvió en una versión anterior.

2. DETALLES:

Las fallas afectan las versiones locales de GMS 9.3.2-SP1 y Analytics 2.5.0.4-R7 y sus respectivas versiones anteriores de ambas. Actualmente, las correcciones están disponibles en las versiones GMS 9.3.3 y Analytics 2.5.2. "El conjunto de vulnerabilidades permite que un atacante vea datos que normalmente no puede recuperar", dijo SonicWall . "Esto podría incluir datos que pertenecen a otros usuarios o cualquier otro dato al que la aplicación pueda acceder. En muchos casos, un atacante puede modificar o eliminar estos datos, lo que provoca cambios persistentes en el contenido o el comportamiento de la aplicación".

La lista de fallas críticas es la siguiente:

- CVE-2023-34124 (puntaje CVSS: 9.4) - Omisión de autenticación de servicio web
- CVE-2023-34133 (puntuación CVSS: 9,8): varios problemas de inyección SQL no autenticados y omisión del filtro de seguridad
- CVE-2023-34134 (puntuación CVSS: 9,8): lectura de hash de contraseña a través del servicio web
- CVE-2023-34137 (puntuación CVSS: 9,4): omisión de autenticación de Cloud App Security (CAS)

Con respecto a lo descubierto por Fortinet sobre la vulnerabilidad de desbordamiento basada en pila [CWE-124] en FortiOS y FortiProxy, se sabe que un atacante remoto puede lograr ejecutar un código o comando arbitrario a través de paquetes diseñados que abordan las políticas de proxy o las políticas de firewall con el modo proxy junto con la inspección profunda de paquetes SSL.

A. Productos afectados:

- Versiones 7.2.0 del FortiOs.
- Versiones 7.2.3 del FortiOs.
- Versiones 7.0.0 del FortiOs.
- Versiones 7.0.10 del FortiOs.

Cabe señalar que la falla no afecta a todas las versiones de FortiOS 6.0, FortiOS 6.2 y FortiOS 6.4, y FortiProxy 1.x y FortiProxy 2.x.

3. RECOMENDACIONES:

- Actualizar a versiones corregidas más nueva, en caso tenga versiones anteriores de GMS y Analytics.
- Deshabilitar la compatibilidad con HTTP/2 en los perfiles de inspección SSL utilizados por las políticas de proxy o las políticas de firewall con modo proxy.
- Actualizar a FortiOS versión 7.4.0 o superior.
- Actualizar a FortiOS versión 7.2.4 o superior.
- Actualizar a FortiOS versión 7.0.11 o superior.
- Actualizar a FortiProxy versión 7.2.3 o superior.
- Actualizar a FortiProxy versión 7.0.10 o superior.

Fuente de Información:	• hxxps://thehackernews.com/2023/07/new-vulnerabilities-disclosed-in.html • hxxps://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0010 • hxxps://www.fortiguard.com/psirt/FG-IR-23-183