SonicWall instó el miércoles a los usuarios de Global Management System (GMS), un software de gestión de firewalls, y del motor de informes de red Analytics, a aplicar las últimas correcciones para protegerse contra un conjunto de 15 vulnerabilidades de seguridad que podrían ser aprovechadas por un actor de amenazas para eludir la autenticación y acceder a información sensible.

De las 15 deficiencias (rastreadas desde CVE-2023-34123 hasta CVE-2023-34137), cuatro tienen una calificación crítica, cuatro tienen una calificación alta y siete tienen una calificación media en cuanto a su gravedad. Estas vulnerabilidades fueron divulgadas por NCC Group.

Las fallas afectan a las versiones locales de GMS 9.3.2-SP1 y anteriores, y Analytics 2.5.0.4-R7 y anteriores. Las correcciones están disponibles en las versiones GMS 9.3.3 y Analytics 2.5.2.

> *«Este conjunto de vulnerabilidades permite a un atacante ver datos a los que normalmente no tendría acceso. Esto podría incluir datos de otros usuarios o cualquier otro dato al que la aplicación misma 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»,* afirmó SonicWall.

La lista de fallas críticas es la siguiente:

- CVE-2023-34124 (puntuación CVSS: 9.4) – Bypass de autenticación en el servicio web.
- CVE-2023-34133 (puntuación CVSS: 9.8) – Múltiples problemas de inyección SQL no autenticada y bypass del filtro de seguridad.
- CVE-2023-34134 (puntuación CVSS: 9.8) – Lectura del hash de contraseñas a través del servicio web.
- CVE-2023-34137 (puntuación CVSS: 9.4) – Bypass de autenticación en Cloud App Security (CAS).

Esta divulgación se produce después de que Fortinet revelara una falla crítica que afecta a FortiOS y FortiProxy (CVE-2023-33308, puntuación CVSS: 9.8) y que podría permitir que un adversario logre la ejecución remota de código en ciertas circunstancias. La compañía afirmó que el problema se resolvió en una versión anterior, sin proporcionar un aviso oficial.

> *«Se ha detectado una vulnerabilidad de desbordamiento de pila [CWE-124] en FortiOS y FortiProxy que podría permitir que un atacante remoto ejecute código o comandos arbitrarios a través de paquetes manipulados que alcanzan políticas de proxy o políticas de firewall con el modo de proxy junto con la inspección profunda de paquetes SSL»,* explicó la compañía en un aviso.

Los productos impactados abarcan desde las versiones 7.2.0 hasta 7.2.3 y desde las versiones 7.0.0 hasta 7.0.10 de FortiOS, así como las versiones 7.2.0 hasta 7.2.2 y 7.0.0 hasta 7.0.9 de FortiProxy. A continuación, se detallan las versiones que solucionan esta vulnerabilidad de seguridad:

- FortiOS versión 7.4.0 o superior.
- FortiOS versión 7.2.4 o superior.
- FortiOS versión 7.0.11 o superior.
- FortiProxy versión 7.2.3 o superior.
- FortiProxy versión 7.0.10 o superior.

Es importante destacar que esta falla no afecta a todas las versiones de FortiOS 6.0, FortiOS 6.2, FortiOS 6.4, FortiProxy 1.x y FortiProxy 2.x.

Para aquellos clientes que no puedan aplicar las actualizaciones de manera inmediata, Fortinet recomienda desactivar el soporte de HTTP/2 en los perfiles de inspección SSL utilizados por las políticas de proxy o las políticas de firewall en modo de proxy.