La compañía de seguridad de redes SonicWall, implementó el viernes correcciones para mitigar una vulnerabilidad crítica de inyección SQL (SQLi) que afecta a sus productos Analytics On-Prem y Global Management System (GMS).

La vulnerabilidad, rastreada como CVE-2022-22280, con una gravedad de 9.4 en el sistema de puntuación CVSS, se deriva de lo que la empresa describe como una *«neutralización inadecuada de elementos especiales»* utilizada en un comando SQL que podría conducir a una inyección SQL no autenticada.

> *«Sin la eliminación o citación suficientes de la sintaxis SQL en las entradas controlables por el usuario, la consulta SQL generada puede hacer que esas entradas se interpreten como SQL en lugar de datos de usuario ordinarios»,* dijo MITRE en su descripción de la inyección SQL.

> *«Esto se puede usar para alterar la lógica de consulta para eludir los controles de seguridad, o para insertar declaraciones adicionales que modifican la base de datos de back-end, posiblemente incluyendo la ejecución de comandos del sistema».*

A H4lo y Catalpa de DBappSecurity HAT Lab, se les atribuye el descubrimiento y notificación de las vulnerabilidades que afectan a 2.5.0.3-2520 y versiones anteriores de Analytics On-Prem, así como a todas las versiones de GMS anteriores a 9.3.1-SP2-Hotfix1.

Se recomienda a las organizaciones que dependen de dispositivos vulnerables que actualicen a Analytics 2.5.0.3-2520-Hotfix y GMS 9.3.1-SP2-Hotfix-2.

> *«No hay una solución disponible para esta vulnerabilidad. Sin embargo, la probabilidad de explotación puede reducirse significativamente al incorporar un Firewall de aplicaciones web (WAF) para bloquear los intentos de SQLi»*, dijo

> SonicWall.