La Fundación Apache (ASF) ha publicado actualizaciones de seguridad para corregir una vulnerabilidad crítica en Traffic Control. Esta falla podría permitir a un atacante ejecutar comandos SQL arbitrarios en la base de datos si se aprovecha con éxito.

La vulnerabilidad de inyección SQL, catalogada como CVE-2024-45387, cuenta con una calificación de 9.9 sobre 10 en el sistema de puntuación CVSS.

> *«Un problema de inyección SQL en Traffic Ops de Apache Traffic Control, presente en las versiones <= 8.0.1 y >= 8.0.0, permite a un usuario con privilegios y roles como 'admin,' 'federation,' 'operations,' 'portal' o 'steering' ejecutar consultas SQL arbitrarias enviando una solicitud PUT especialmente diseñada»,* explicaron los responsables del proyecto en un comunicado.

Apache Traffic Control es una solución de código abierto para implementar Redes de Distribución de Contenido (CDN). En junio de 2018, fue reconocido como un proyecto de nivel superior (TLP) por la ASF.

El investigador Yuan Luo, del Laboratorio de Seguridad Tencent YunDing, ha sido acreditado por identificar y reportar esta vulnerabilidad, que ya ha sido corregida en la versión Apache Traffic Control 8.0.2.

Este avance coincide con la resolución de una vulnerabilidad de omisión de autenticación en Apache HugeGraph-Server (CVE-2024-43441), que afectaba a las versiones entre la 1.0 y la 1.3. Este problema se solucionó con la versión 1.5.0.

Asimismo, la ASF también lanzó un parche para una vulnerabilidad significativa en Apache Tomcat (CVE-2024-56337), que podría permitir la ejecución remota de código (RCE) bajo ciertas circunstancias.

Se aconseja a los usuarios actualizar sus sistemas a las versiones más recientes del software para mitigar posibles riesgos de seguridad.