Un investigador de ciberseguridad publicó recientemente los detalles y prueba de concepto sobre una vulnerabilidad zero-day sin parches en phpMyAdmin, una de las aplicaciones más populares para administrar bases de datos MySQL y MariaDB.

phpMyAdmin es una herramienta administradora gratuita y de código abierto para MySQL y MariaDB, que se utiliza ampliamente para administrar las bases de datos de sitios web creados con sistemas gestores de contenido como WordPress, Joomla, y muchos más.

Descubierta por el investigador y pentester Manuel García Cárdenas, la vulnerabilidad sería una falla de falsificación de solicitudes entre sitios (CSRF), también conocida como XSRF, un ataque conocido en el que los hackers engañan a los usuarios autenticados para que ejecuten una acción no deseada.

Identificada como CVE-2019-12922, la falla recibió una calificación media debido a su alcance limitado que solo permite que un atacante elimine cualquier servidor configurado en la página de configuración un panel phpMyAdmin en el servidor de la víctima.

Sin embargo, no es algo muy preocupante, ya que el ataque no permite a los atacantes eliminar bases de datos o tablas almacenadas en el servidor.

Todo lo que un atacante debe hacer es enviar una URL diseñada a los administradores web específicos, que ya han iniciado sesión en su panel phpMyAdmin en el mismo navegador, engañándolos para que eliminen sin saberlo el servidor configurado simplemente haciendo clic en él.

> *«El ataque puede crear fácilmente un hipervínculo falso que contiene la solicitud que desea ejecutar en nombre del usuario, lo que hace posible un ataque CSRF debido al uso incorrecto del método HTTP»*, explicó Cárdenas en una publicación.

Sin embargo, la vulnerabilidad es trivial para explotar, ya que aparte de conocer la URL de un servidor de destino, un atacante no necesita conocer ninguna otra información, como el

nombre de las bases de datos.

Prueba de concepto

La vulnerabilidad afecta a las versiones de phpMyAdmin hasta 4.9.0.1, que es la última versión del software hasta ahora. La falla reside en phpMyAdmin 5.0.0-alpha1, que se lanzó en julio de 2019.

Cárdenas descubrió esta vulnerabilidad en junio de 2019 y también la informó responsablemente a los administradores del proyecto.

Sin embargo, luego de que los mantenedores de phpMyAdmin no pudieron corregir la vulnerabilidad dentro de los 90 días posteriores a la notificación, el investigador decidió divulgar los detalles y PoC al público el pasado 13 de septiembre.

Para abordar la vulnerabilidad, Cárdenas recomendó *«implementar en cada llamada la validación de la variable de token, como ya se hizo en otras solicitudes phpMyAdmin»*, como una solución.