Investigadores de seguridad advirtieron sobre una vulnerabilidad crítica que descubrieron en un plugin popular de WordPress, Live Chat, que al ser explotados, permitirían que hackers remotos no autorizados roben registros de chat o manipulen sesiones de chat.

La vulnerabilidad fue identificada como CVE-2019-12498 y reside en el *«Soporte de Chat en Vivo de WP»*, que actualmente utilizan más de 50,000 empresas para brindar soporte al cliente y chatear con los visitantes por medio de sus sitios web.

Descubierta por los investigadores de Alert Logic, la falla se origina debido a una verificación de validación incorrecta para la autenticación que podría permitir a los usuarios no autenticados acceder a los puntos finales de la API REST restringida.

Según los investigadores, un atacante potencial remoto puede explotar puntos finales expuestos con fines maliciosos que incluyen:

- Robo de todo el historial de chat para todas las cuentas de sesiones de chat
- Modificación o borrado del historial del chat
- Inyección de mensajes en una sesión de chat activa, haciéndose pasar por un agente de atención al cliente
- Finalizar a la fuerza las sesiones de chat activas, como parte de un ataque de denegación de servicio (DoS)

El problema afecta a todos los sitios web de WordPress, y a sus clientes también, que aún utilizan la versión 8.0.32 o anterior de WP Live Chat Support.

Los expertos informaron acerca del problema a los desarrolladores del plugin, que luego lanzaron una versión actualizada y parcheada de su plugin.

Aunque los investigadores no han visto ninguna explotación activa de la falla, se recomienda a los administradores de WordPress que instalen la última versión del complemento tan pronto como sea posible.