Hackers están explotando algunas vulnerabilidades críticas de seguridad en uno de los populares plugins de redes sociales para compartir el control de los sitios web de WordPress que aún ejecutan una versión vulnerable de dicho plugin.

El plugin vulnerable es Social Warfare, que es altamente implementado por más de 900,000 usuarios de WordPress. Se utiliza para agregar botones de redes sociales a un sitio web o blog.

A finales del mes pasado, los encargados de Social Warfare para WordPress lanzaron una versión actualizada 3.5.3 del plugin para parchear dos vulnerabilidades de seguridad: secuencias de comandos entre sitios almacenadas (XSS) y ejecución remota de código (RCE), rastreados por un solo identificados, CVE-2019-9978.

Los hackers pueden explotar las vulnerabilidades para ejecutar código PHP arbitrario y tomar el control completo de sitios web y servidores sin autenticación, para luego utilizar los sitios comprometidos para realizar minería de criptomonedas o alojar código de exploits maliciosos.

Sin embargo, el mismo día en que Social Warfare lanzó la versión parcheada de su complemento, un investigador de seguridad sin nombre publicó una divulgación completa y una prueba de concepto para la vulnerabilidad almacenada de secuencias de comandos entre sitios (XSS).

Poco tiempo después de la divulgación completa y el lanzamiento de PoC, los atacantes comenzaron a intentar explotar la vulnerabilidad, pero afortunadamente, solo se limitó a la actividad de redireccionamiento de JavaScript inyectado, y los investigadores no encontraron intentos de explotar la vulnerabilidad de RCE.

Ahora, los investigadores de la Unidad 42 de la Red de Palo Alto encontraron varios exploits aprovechando estas vulnerabilidades, incluyendo un exploit para la vulnerabilidad RCE que permite al atacante controlar el sitio web afectado y un exploit para la vulnerabilidad XSS que redirige a las víctimas a un sitio de anuncios.

Aunque ambas fallas se originaron debido a un manejo incorrecto de la entrada, el uso de una función incorrecta, insuficiente, eventualmente hizo posible que los atacantes remotos las explotaran sin requerir autenticación.

> *«La causa raíz de cada una de estas dos vulnerabilidades es la misma: el mal uso de la función is_admin() en WordPress. is_admin solo verifica si la página solicitada es parte de la interfaz de administración y no evitará ninguna visita no autorizada»*, dicen los investigadores.

Hasta ahora, más de 37,000 sitios web de WordPress, incluyendo sitios de educación, finanzas y noticias, aún utilizan una versión obsoleta y vulnerable del plugin, dejando a cientos de millones de sus visitantes expuestos.

Ya que es probable que los hackers sigan explotando las vulnerabilidades para atacar a los usuarios de WordPress, se recomienda a los administradores de sitios web actualizar el plugin Social Warfare a la versión 3.5.3 lo más pronto posible.