Cientos de servidores Openfire XMPP presentan una vulnerabilidad recién descubierta de gravedad alta que aún no ha sido corregida y son susceptibles a un nuevo tipo de ataque, según un informe reciente de VulnCheck.

Identificada como CVE-2023-32315 (puntuación CVSS: 7.5), la vulnerabilidad se refiere a un fallo de seguridad relacionado con la expansión de rutas en la consola administrativa de Openfire, lo que podría permitir a un atacante no autenticado acceder a páginas que normalmente están reservadas para usuarios con privilegios.

Esta vulnerabilidad afecta a todas las versiones del software lanzadas desde abril de 2015, comenzando con la versión 3.10.0. El desarrollador, Ignite Realtime, la solucionó a principios de mayo con el lanzamiento de las versiones 4.6.8, 4.7.5 y 4.8.0.

Los responsables del mantenimiento del software explicaron en un detallado informe que *«ya se habían implementado medidas de protección contra este tipo de ataque de expansión de rutas, pero estas no defendían contra ciertas codificaciones no estándar de URL para caracteres UTF-16 que no eran compatibles con el servidor web integrado utilizado en ese momento».*

> *«Una actualización posterior del servidor web integrado incluyó soporte para codificaciones no estándar de URL de caracteres UTF-16. Sin embargo, las medidas de protección contra la expansión de rutas en Openfire no se actualizaron para incluir protección contra esta nueva codificación».*

Como resultado, un atacante podría aprovechar esta debilidad para eludir los requisitos de autenticación en las páginas de la consola de administración. Desde entonces, se ha observado la explotación activa de esta vulnerabilidad en la naturaleza, incluso por parte de atacantes relacionados con el malware del botnet criptográfico Kinsing (también conocido como Money Libra).

Un escaneo realizado por la firma de ciberseguridad Shodan revela que, de los más de 6,300

servidores Openfire accesibles en Internet, aproximadamente la mitad de ellos está utilizando versiones afectadas de esta solución XMPP de código abierto.

Aunque los exploits públicos han aprovechado la vulnerabilidad para crear un usuario administrativo, iniciar sesión y luego cargar un complemento para lograr la ejecución de código, VulnCheck afirmó que es posible hacerlo sin necesidad de crear una cuenta de administrador, lo que lo hace más sigiloso y atractivo para los actores maliciosos.

El investigador de seguridad Jacob Baines, al profundizar en la forma en que operan los exploits existentes, explicó que *«implican la creación de un usuario administrativo para acceder a la interfaz de complementos de Openfire».*

> *«El sistema de complementos permite a los administradores agregar funcionalidades prácticamente arbitrarias a Openfire mediante la carga de archivos JAR de Java. Esto es, sin duda, un punto de partida para pasar de la elusión de la autenticación a la ejecución de código a distancia».*

Por otro lado, el método mejorado y menos evidente desarrollado por VulnCheck utiliza un enfoque sin la necesidad de un usuario y extrae el JSESSIONID y el token CSRF al acceder a una página llamada 'plugin-admin.jsp' y luego carga el complemento JAR mediante una solicitud POST.

> Baines explicó que *«sin autenticación, el complemento es aceptado e instalado. La shell web luego se puede acceder sin autenticación, aprovechando la expansión de rutas».*

> *«Este enfoque evita que los intentos de inicio de sesión queden registrados en el registro de auditoría de seguridad y previene que se registre la notificación de*

> *‘complemento cargado’. Esto es significativo ya que no deja evidencia en el registro de auditoría de seguridad».*

La única señal reveladora de que algo malicioso está ocurriendo son los registros capturados en el archivo openfire.log, que un adversario podría eliminar utilizando la CVE-2023-32315, advirtió la compañía.

Dado que la vulnerabilidad ya está siendo explotada en ataques del mundo real, se recomienda encarecidamente a los usuarios que actualicen a las últimas versiones lo más rápido posible para protegerse contra posibles amenazas.