Los expertos en seguridad han descubierto un intento de asalto «creíble» dirigido a la Fundación OpenJS de una manera que recuerda al incidente recientemente descubierto dirigido al proyecto de código abierto XZ Utils.

> *«El Consejo de Proyectos Cruzados de la Fundación OpenJS recibió una serie de correos electrónicos sospechosos con mensajes similares, pero con diferentes nombres y correos electrónicos asociados a GitHub que se solapaban»,* comunicaron en una alerta conjunta la Fundación OpenJS y la Fundación de Seguridad de Código Abierto (OpenSSF).

Según Robin Bender Ginn, directora ejecutiva de la Fundación OpenJS, y Omkhar Arasaratnam, gerente general de OpenSSF, los correos electrónicos instaban a OpenJS a tomar medidas para actualizar uno de sus populares proyectos de JavaScript para remediar vulnerabilidades críticas sin dar detalles específicos.

El o los autores de los correos electrónicos también solicitaron a OpenJS que los designara como nuevos responsables del proyecto, a pesar de tener escasa participación previa. Se dice que otros dos populares proyectos de JavaScript que no son alojados por OpenJS también fueron objeto de actividades similares.

Sin embargo, ninguna de las personas que contactaron a OpenJS recibió acceso privilegiado al proyecto alojado por OpenJS.

El incidente pone de relieve la forma en que el único responsable de XZ Utils fue atacado por identidades ficticias creadas específicamente para lo que se cree que es una campaña de ingeniería social y presión diseñada para convertir a Jia Tan (también conocido como JiaT75) en co-responsable del proyecto.

Esto sugiere que el intento de sabotaje a XZ Utils podría no ser un incidente aislado y formar parte de una campaña más amplia para socavar la seguridad de varios proyectos, afirmaron los dos grupos de código abierto. No se revelaron los nombres de los proyectos de JavaScript.

Hasta ahora, Jia Tan no tiene otras huellas digitales aparte de sus contribuciones, lo que sugiere que la cuenta fue creada únicamente para ganar credibilidad en la comunidad de desarrollo de código abierto a lo largo del tiempo y, en última instancia, introducir discretamente una puerta trasera en XZ Utils.

También sirve para señalar la sofisticación y paciencia que se han invertido en planificar y ejecutar la campaña al atacar un proyecto de código abierto dirigido por voluntarios que se utiliza en muchas distribuciones de Linux, poniendo en riesgo a organizaciones y usuarios frente a ataques a la cadena de suministro.

El incidente de la puerta trasera de XZ Utils también destaca la «fragilidad» del ecosistema de código abierto y los riesgos creados por el agotamiento de los responsables, según señaló la Agencia de Ciberseguridad e Infraestructura de EE. UU. (CISA) la semana pasada.

> *«La responsabilidad de la seguridad no debería recaer en un único responsable de código abierto, como ocurrió en este caso con efectos casi desastrosos»,* indicaron los funcionarios de CISA Jack Cable y Aeva Black.
>
> *«Cada fabricante tecnológico que se beneficie del software de código abierto debe cumplir con su parte siendo consumidores responsables y contribuyentes sostenibles a los paquetes de código abierto en los que confían».*

La entidad recomienda que los fabricantes de tecnología y los operadores de sistemas que incorporen componentes de código abierto deberían, ya sea directamente o mediante apoyo a los mantenedores, realizar auditorías periódicas al código fuente, eliminar categorías completas de vulnerabilidades e implementar otros principios de seguridad por diseño.

> *«Estos ataques de ingeniería social están aprovechando el sentido de responsabilidad que los mantenedores tienen con su proyecto y comunidad para*

> *influenciarlos»*, señalaron Bender Ginn y Arasaratnam.
>
> *«Observa cómo te hacen sentir las interacciones. Las interacciones que generan dudas sobre uno mismo, sentimientos de insuficiencia, de no estar contribuyendo lo suficiente al proyecto, etc., podrían formar parte de un ataque de ingeniería social».*