Red Hat emitió el viernes una *«alerta de seguridad urgente»* advirtiendo que dos versiones de una conocida biblioteca de compresión de datos llamada XZ Utils (anteriormente conocida como LZMA Utils) han sido contaminadas con código malicioso diseñado para permitir acceso remoto no autorizado.

Este incidente de compromiso en la cadena de suministro de software, identificado como CVE-2024-3094, tiene una calificación CVSS de 10.0, lo que indica una gravedad máxima. Afecta a las versiones 5.6.0 (lanzada el 24 de febrero) y 5.6.1 (lanzada el 9 de marzo) de XZ Utils.

> *«A través de una serie de complicadas técnicas de ocultamiento, el proceso de construcción de la biblioteca liblzma extrae un archivo de objeto preconstruido de un archivo de prueba camuflado presente en el código fuente, el cual es luego empleado para alterar funciones específicas en el código de liblzma»,* informó la subsidiaria de IBM en un comunicado.
>
> *«Esto resulta en una versión modificada de la biblioteca liblzma que puede ser utilizada por cualquier software vinculado a esta biblioteca, interceptando y modificando la interacción de datos con la misma»*.

El código malicioso incrustado en la biblioteca está diseñado específicamente para interferir con el proceso del demonio sshd para SSH (Secure Shell) a través del conjunto de software systemd, y potencialmente permitir que un atacante rompa la autenticación de sshd y obtenga acceso no autorizado al sistema de forma remota *«en las circunstancias adecuadas».*

El investigador de seguridad de Microsoft, Andrés Freund, ha sido reconocido por descubrir y reportar este problema el viernes. Se afirma que el código malicioso, altamente encubierto, fue introducido a lo largo de una serie de cuatro compromisos en el Proyecto Tukaani en GitHub por un usuario identificado como Jia Tan (JiaT75).

> *«Dada la actividad durante varias semanas, el autor de los compromisos está o bien directamente involucrado o ha habido algún tipo de compromiso severo de su sistema. Lamentablemente, la segunda opción parece menos probable, dado que se comunicaron en varias listas sobre las 'correcciones'»*, señaló Freund.

GitHub, propiedad de Microsoft, ha desactivado temporalmente el repositorio de XZ Utils mantenido por el Proyecto Tukaani *«debido a una violación de los términos de servicio de GitHub».* Actualmente, no se han reportado casos de explotación activa en el entorno real.

La evidencia indica que los paquetes afectados están presentes solamente en Fedora 41 y Fedora Rawhide, y no afectan a Red Hat Enterprise Linux (RHEL), Debian Stable, Amazon Linux y SUSE Linux Enterprise y Leap.

Como medida preventiva, se ha sugerido a los usuarios de Fedora Linux 40 que regresen a una versión 5.4. Algunas otras distribuciones de Linux impactadas por este ataque en la cadena de suministro son:

- Kali Linux (entre el 26 y el 29 de marzo)
- openSUSE Tumbleweed y openSUSE MicroOS (entre el 7 y el 28 de marzo)
- Versiones de prueba, inestables y experimentales de Debian (desde 5.5.1alpha-0.1 hasta 5.6.1-1)

Este incidente ha llevado a la Agencia de Ciberseguridad e Infraestructura de EE. UU. (CISA) a emitir su propia alerta, instando a los usuarios a regresar a una versión no comprometida de XZ Utils (por ejemplo, XZ Utils 5.4.6 Estable).