INCIDENTE DE XZ UTILS

Borja Torres Hernández
Diego Pastrana Monzón

Índice

Definición:

Una puerta trasera (en este caso), es un tipo de vulnerabilidad o de programa malicioso que otorga acceso no autorizado a un sistema informático, eludiendo los mecanismos de seguridad normales. Este acceso puede permitir a los atacantes ejecutar comandos, manipular datos o tomar control del sistema afectado.

Mecanismo de infección o propagación:

El método de propagación las puertas traseras pueden ser de muchas formas diferentes. En muchos casos, se usa ingeniería social para engañar a las víctimas así conseguir que instalen un software malicioso o que ejecuten comandos para lograr tener acceso remoto.

Otra forma bastante común es infiltrarse en el desarrollo del software, ahí los atacantes modifican proyectos oficiales /legítimos para incluir código malicioso sin que nadie se de cuenta, entonces lo distribuyen como parte de actualizaciones o como una descarga oficial.

También se pueden explotar vulnerabilidades en aplicaciones o en sistemas para introducir una puerta trasera de forma automática, sin que el usuario se de cuenta. Además, en algunos casos se propagan a través de archivos maliciosos/infectados en correos electrónicos o descargas desde sitios webs de dudosa reputación.

Mecanismo de reparación:

Primero hay que identificar y eliminar el malware mediante herramientas de análisis que detecten los archivos y configuraciones que están comprometidos. Una vez ya lo hemos eliminado, se deben instalar versiones actualizadas y totalmente limpias del software afectado (como por ejemplo el sistema operativo) para que de esta manera nos aseguremos de la integridad del sistema.

Además, es importante realizar auditorías de seguridad para comprobar que no existan otros fallos o vulnerabilidades que puedan ser explotadas. Por último, se deben implementar medidas preventivas como el uso de firmas digitales, configuraciones de acceso con más restricciones y también monitoreo continuo para poder evitar infecciones futuras.

También deberíamos de establecer una jerarquía entre diferentes usuarios teniendo en cuenta el nivel de acceso que debería tener cada uno. De esta manera podemos evitar que en caso de hackeo de cualquiera de ellos podemos minimizar los daños debido a que no van a tener permisos para determinados elementos críticos del sistema.

Analiza los ataques y medios de infección que han sucedido, así como las soluciones empleadas:

El ataque al proyecto XZ Utils se llevó a cabo mediante una estrategia de ingeniería social muy planificada. El atacante, que se hacia llamar Jia Tan, inició su acercamiento en noviembre de 2021 enviando un parche al proyecto libarchive, el cual contenía código inseguro que fue fusionado sin mayor discusión. Este movimiento inicial sirvió como prueba para evaluar la facilidad de introducir código malicioso en proyectos de código abierto. Posteriormente, en 2022, Jia Tan dirigió su atención a XZ Utils, enviando un parche que, aunque no era muy significativo en contenido, todo formaba parte de su estrategia para ganarse la confianza del mantenedor principal, que se llamaba Lasse Collin. Para presionar la aceptación del parche, aparecieron otros usuarios desconocidos que instaban a Collin a aprobarlo, sugiriendo que, debido al lento calendario de lanzamientos, la comunidad tardaría años en beneficiarse de nuevas características. Esta presión coordinada buscaba debilitar la resistencia del mantenedor y facilitar la infiltración del atacante en el proyecto.

Una vez que Jia Tan logró establecerse como un colaborador de fiar , introdujo código malicioso en XZ Utils. Este código fue posteriormente compilado y distribuido como una versión oficial en los servidores de Debian y Red Hat. Como resultado, los usuarios que actualizaron sus sistemas desde estos repositorios oficiales descargaron la versión comprometida de la librería liblzma. El malware incorporado permitía a los atacantes interceptar conexiones SSH y ejecutar comandos de forma remota en los sistemas afectados, comprometiendo gravemente la seguridad de innumerables servidores y estaciones de trabajo.

La detección del ataque se produjo el 29 de marzo, cuando un ingeniero de Microsoft, durante tareas rutinarias, identificó actividades sospechosas en XZ Utils. Esto desencadenó una respuesta inmediata de la comunidad de código abierto. Se alertó a los usuarios a través de los canales oficiales, se suspendió la cuenta de Jia Tan y se revirtieron los cambios maliciosos en el proyecto. Además, se lanzó una actualización limpia de XZ Utils y se llevaron a cabo auditorías de seguridad para garantizar la integridad del software. Este incidente destacó la importancia de fortalecer la seguridad en proyectos críticos de software de código abierto, especialmente aquellos mantenidos por individuos o pequeños equipos sin recursos suficientes.

Como medida preventiva para futuros ataques a la cadena de suministro, se implementaron procesos más rigurosos para aceptar nuevas contribuciones. Esto incluyó una revisión más estricta del código, la firma digital de los commits y procedimientos más exigentes para la incorporación de nuevos colaboradores. El ataque evidenció cómo una librería esencial, mantenida por una sola persona y sin actualizaciones durante años, puede convertirse en un objetivo vulnerable. La comunidad reconoció la necesidad de apoyar y financiar adecuadamente estos proyectos para mantener la seguridad y estabilidad del ecosistema de software de código abierto.

Conclusión:

Teniendo en cuenta el desarrollo de este caso, hemos aprendido que no siempre es recomendable tener la última versión de un software y tener especial cuidado en que no seamos víctimas de ingeniería social.

Además, es muy recomendable que a la hora de realizar cualquier actualización o instalación revisemos las últimas notas sobre la versión y verifiquemos en internet si ha habido alguna vulnerabilidad o problema serio.

Si tenemos cualquier duda acerca del funcionamiento del software que vamos a instalar deberíamos abrir un canal de comunicación con el equipo de soporte si lo tiene o en caso contrario, intentar comunicarnos con los propios desarrolladores.

Bibliografía:

EDteam
https://ed.team/blog/el-hackeo-a-linux-que-casi-colapsa-internet-toda-la-historia

Nate Gentile
https://youtu.be/mTpDmhF4BSw