Universidad Autónoma de Baja California
Facultad de Ciencias Químicas e Ingeniería

Plan de Ingeniero en Software y Tecnologías Emergentes

Materia
Seguridad del Software(371)

Meta 4.1.2
Listas de vulnerabilidades y debilidades en software

Docente
Carlos Francisco Alvarez Salgado

Participante:
Luis Eduardo Galindo Amaya (1274895)

Tijuana, 12. abril 2024

Documentar la vulnerabilidad

CVE-2024-3094

Descripcion

Se encontró código malicioso en los archivos de xz a partir de la versión 5.6.0. Este código manipula la construcción de liblzma para modificar su funcionalidad, lo que afecta a cualquier software que utilice esta biblioteca al interceptar y modificar la interacción de datos.

Análisis técnico del backdoor

El código malicioso se integra en el servidor OpenSSH (proceso sshd), aprovechando que liblzma es un componente requerido en algunas versiones de OpenSSH. El flujo para ejecutar el payload enviado por el atacante sigue estos pasos:

1. El código malicioso intercepta la función RSA_public_decrypt, originalmente utilizada para la validación de firmas RSA.
2. Cuando un cliente SSH se conecta, el código malicioso obtiene el valor de N dentro de la estructura RSA.
3. Luego, los últimos 240 bytes del valor "N" se descifran utilizando el algoritmo ChaCha20 con una clave de descifrado incluida en el código malicioso.
4. Se verifica la validez de una firma de 114 bytes incluida en los datos descifrados utilizando el algoritmo de firma asimétrica de curva elíptica Ed448.
5. Si la firma es válida, se ejecuta el comando contenido en el texto directamente a través de system().
6. En caso de un payload inválido, el backdoor continúa la ejecución de la función RSA_public_decrypt de manera transparente y descarta el comando recibido.

Conclusión

Durante esta investigación aprendí como funciona la vulnerabilidad CVE-2024-3094, este es una de las vulnerabilidades más series en los últimos meses, el hecho de que sea en un proyecto con su código disponible permitió encontrar esta vulnerabilidad rápidamente.

Fuentes

1. Administrador. (2024, April 9). *CVE-2024-3094: Backdoor en librería xz utils*. Tarlogic Security. https://www.tarlogic.com/es/blog/cve-2024-3094-backdoor-xz-utils/
2. *CVE-2024-3094 Detail*. NVD. (n.d.). https://nvd.nist.gov/vuln/detail/CVE-2024-3094