Se han identificado seis vulnerabilidades de seguridad en la conocida herramienta Rsync, utilizada para sincronización de archivos en sistemas Unix. Algunas de estas fallas permiten a los atacantes ejecutar código arbitrario en los clientes afectados.

> *«Los atacantes podrían controlar un servidor malicioso y acceder o modificar archivos arbitrarios de los clientes conectados. Esto incluye la posibilidad de extraer datos sensibles, como claves SSH, y ejecutar código malicioso sobrescribiendo archivos como `~/.bashrc` o `~/.popt`«,* informó el Centro de Coordinación CERT (CERT/CC) en un comunicado.

Estas vulnerabilidades incluyen desbordamiento de memoria, fuga de información, exposición de archivos, escritura en directorios no autorizados y condiciones de carrera relacionadas con enlaces simbólicos. Los detalles son los siguientes:

- CVE-2024-12084 (CVSS: 9.8): Desbordamiento de memoria en el montón debido a un manejo incorrecto de la longitud del checksum en Rsync.
- CVE-2024-12085 (CVSS: 7.5): Fuga de información causada por el uso de contenido no inicializado en la pila.
- CVE-2024-12086 (CVSS: 6.1): El servidor Rsync permite la exposición de archivos arbitrarios de los clientes.
- CVE-2024-12087 (CVSS: 6.5): Vulnerabilidad de recorrido de rutas en Rsync.
- CVE-2024-12088 (CVSS: 6.5): Salto de restricciones en la opción `--safe-links`, permitiendo recorridos de rutas.
- CVE-2024-12747 (CVSS: 5.6): Condición de carrera en la gestión de enlaces simbólicos por parte de Rsync.

Simon Scannell, Pedro Gallegos y Jasiel Spelman, del equipo de Investigación de Vulnerabilidades de Google Cloud, han sido reconocidos por descubrir las primeras cinco vulnerabilidades. Aleksei Gorban, investigador independiente, identificó el problema relacionado con las condiciones de carrera.

> *«En el caso más crítico, identificado como CVE-2024-12084, un atacante solo necesita acceso de lectura anónima a un servidor Rsync, como un repositorio público, para ejecutar código arbitrario en el sistema que ejecuta el servidor»*, explicó Nick Tait, de Red Hat Product Security.

CERT/CC también señaló que las vulnerabilidades CVE-2024-12084 y CVE-2024-12085 pueden combinarse para permitir la ejecución de código arbitrario en clientes que ejecuten un servidor Rsync.

Las actualizaciones para resolver estas vulnerabilidades están disponibles en la versión 3.4.0 de Rsync, lanzada hoy. Para quienes no puedan actualizar, se sugieren las siguientes mitigaciones:

- CVE-2024-12084: Desactivar el soporte para algoritmos SHA compilando con `CFLAGS=-DDISABLE_SHA512_DIGEST` y `CFLAGS=-DDISABLE_SHA256_DIGEST`.
- CVE-2024-12085: Compilar utilizando la opción `-ftrivial-auto-var-init=zero`, que inicializa automáticamente el contenido de la pila con ceros.