



Vulnerabilidad de Serv-U en SolarWinds se encuentra bajo ataque activo

Una vulnerabilidad de alta gravedad recientemente parcheada que afecta al software de transferencia de archivos SolarWinds Serv-U está siendo activamente explotada por actores maliciosos en el entorno.

La vulnerabilidad, identificada como CVE-2024-28995 (puntuación CVSS: 8.6), se trata de un [error](#) de transversalidad de directorios que podría permitir a los atacantes acceder a archivos sensibles en el servidor afectado.

Esta vulnerabilidad afecta a todas las versiones del software anteriores e incluyendo la Serv-U 15.4.2 HF 1, y fue corregida por la compañía en la versión [Serv-U 15.4.2 HF 2](#) (15.4.2.157) lanzada a principios de este mes.

Los productos afectados por CVE-2024-28995 son los siguientes:

- Serv-U FTP Server 15.4
- Serv-U Gateway 15.4
- Serv-U MFT Server 15.4
- Serv-U File Server 15.4

El investigador de seguridad Hussein Daher de Web Immunify ha sido reconocido por descubrir y reportar esta vulnerabilidad. Tras la divulgación pública, se han publicado [detalles técnicos](#) adicionales y un exploit de [prueba de concepto](#) (PoC).

La firma de ciberseguridad Rapid7 describió la vulnerabilidad como fácil de explotar, permitiendo a atacantes externos no autenticados leer cualquier archivo en el disco, incluyendo archivos binarios, siempre que conozcan la ruta del archivo y éste no esté bloqueado.

«Problemas de divulgación de información de alta gravedad como CVE-2024-28995 pueden ser utilizados en ataques rápidos donde los atacantes obtienen acceso y tratan de exfiltrar rápidamente datos de soluciones de transferencia de archivos



con el objetivo de extorsionar a las víctimas», [señaló la compañía](#).

«Los productos de transferencia de archivos han sido objetivo de una amplia gama de adversarios en los últimos años, incluyendo grupos de ransomware.»

De hecho, según la firma de inteligencia de amenazas GreyNoise, actores maliciosos ya han comenzado a realizar [ataques oportunistas](#) explotando esta vulnerabilidad contra sus servidores honeypot para acceder a archivos sensibles como /etc/passwd, con intentos registrados también desde China.

Dado que fallas anteriores en el software Serv-U han sido explotadas por actores maliciosos, es crucial que los usuarios apliquen las actualizaciones lo antes posible para mitigar posibles amenazas.

«El hecho de que los atacantes estén utilizando PoCs disponibles públicamente significa que la barrera de entrada para los actores maliciosos es extremadamente baja», comentó Naomi Buckwalter, directora de seguridad de productos en Contrast Security.

«La explotación exitosa de esta vulnerabilidad podría ser un punto de partida para los atacantes. Al obtener acceso a información sensible como credenciales y archivos del sistema, los atacantes pueden utilizar esa información para lanzar ataques adicionales, una técnica conocida como 'encadenamiento'. Esto puede llevar a un mayor compromiso, afectando potencialmente a otros sistemas y aplicaciones.»