SolarWinds ha publicado actualizaciones para corregir cuatro vulnerabilidades críticas de seguridad en su software de transferencia de archivos Serv-U que, de ser explotadas con éxito, podrían permitir la ejecución remota de código.

Las fallas, todas con una puntuación de 9.1 en el sistema CVSS, se detallan a continuación:

- CVE-2025-40538 – Vulnerabilidad de control de acceso deficiente que posibilita a un atacante crear un usuario administrador del sistema y ejecutar código arbitrario como root aprovechando privilegios de administrador de dominio o de grupo.
- CVE-2025-40539 – Vulnerabilidad de confusión de tipos que permite a un atacante ejecutar código nativo arbitrario como root.
- CVE-2025-40540 – Vulnerabilidad de confusión de tipos que permite a un atacante ejecutar código nativo arbitrario como root.
- CVE-2025-40541 – Vulnerabilidad de referencia directa insegura a objetos (IDOR) que posibilita a un atacante ejecutar código nativo como root.

SolarWinds indicó que estas vulnerabilidades requieren privilegios administrativos para poder ser explotadas con éxito. Asimismo, señaló que representan un riesgo de seguridad medio en implementaciones sobre Windows, ya que los servicios *«suelen ejecutarse por defecto bajo cuentas con privilegios limitados»*.

Las cuatro vulnerabilidades afectan a SolarWinds Serv-U 15.5 y han sido corregidas en SolarWinds Serv-U 15.5.4.

Aunque SolarWinds no ha confirmado que estas fallas estén siendo explotadas activamente, vulnerabilidades anteriores en el mismo software (CVE-2021-35211, CVE-2021-35247 y CVE-2024-28995) sí fueron aprovechadas por actores maliciosos, incluido un grupo de origen chino identificado como Storm-0322 (anteriormente denominado DEV-0322).