Date Posted: 2026/03/03

[Vulnerability Alert] 4 Critical Security Vulnerabilities Found in SolarWinds Serv-U

- Subject Explanation: [Vulnerability Alert] 4 Critical Security Vulnerabilities Found in SolarWinds Serv-U

- Content Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202602-00000015
  - SolarWinds Serv-U is a server software for secure file transfer, supporting multiple protocols such as FTP, FTPS, and SFTP. It features an easy-to-use management interface and supports cross-platform and cross-device access. Recently, SolarWinds released an advisory regarding 4 critical security vulnerabilities in its Serv-U product.
  - [CVE-2025-40538, CVSS: 9.1] This is an access control vulnerability that allows an attacker to create a system administrator and execute arbitrary code as a privileged account through domain administrator or group administrator privileges.
  - [CVE-2025-40539, CVSS: 9.1] This is a type confusion vulnerability that allows an attacker to execute arbitrary local code as a privileged account.
  - [CVE-2025-40540, CVSS: 9.1] This is a type confusion vulnerability that allows an attacker to execute arbitrary local code as a privileged account.
  - [CVE-2025-40541, CVSS: 9.1] This is an Insecure Direct Object Reference (IDOR) vulnerability that allows an attacker to execute arbitrary local code as a privileged account.
- Impacted Platforms:
  - SolarWinds Serv-U 15.5 version
- Suggested Measures:
  - Please update to the following versions: SolarWinds Serv-U 15.5.4 and later versions

---

Computer and Communication Center
Network Systems Division