

Posted Date: 2025/11/26

[Vulnerability Alert] SolarWinds Serv-U Software Has 3 Critical Security Vulnerabilities (CVE-2025-40547)(CVE-2025-40548)(CVE-2025-40549)

- Subject: [Vulnerability Alert] SolarWinds Serv-U Software Has 3 Critical Security Vulnerabilities (CVE-2025-40547)(CVE-2025-40548)(CVE-2025-40549)
- Content:
 - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center Security Alert TWCERTCC-200-202511-00000016
 - SolarWinds Serv-U is server software used 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 issued an advisory stating that its Serv-U product has 3 critical security vulnerabilities.
 - [CVE-2025-40547, CVSS: 9.1] This is a logic error vulnerability, which may allow an attacker with administrator privileges to execute code.
 - [CVE-2025-40548, CVSS: 9.1] This is a missing validation vulnerability, which may allow an attacker with administrator privileges to execute code.
 - [CVE-2025-40549, CVSS: 9.1] This is a path restriction bypass vulnerability, which may allow an attacker with administrator privileges to execute code on the directory.
- Affected Platforms:
 - SolarWinds Serv-U version 15.5.2.2.102
- Recommended Measures:
 - Please update to the following version: SolarWinds Serv-U version 15.5.3
- References:
 1. <https://www.twcert.org.tw/tw/cp-169-10519-a28f7-1.html>

Computer and Communications Center
Network Systems Group

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20251126_02



Last update: **2025/11/26 11:18**