SolarWinds Serv-U Broken Access Control Remote Code Execution Vulnerability (CVE-2025-40538)

Security Advisory Summary

A broken access control vulnerability exists in Serv-U which when exploited together, gives a malicious actor the ability to create a system admin user and execute arbitrary code as a privileged account via domain admin or group admin privileges.

This issue requires administrative privileges to abuse. On Windows deployments, the risk is scored as a medium because services frequently run under less-privileged service accounts by default.

Affected Products

- SolarWinds Serv-U 15.5

Fixed Software Release

- SolarWinds Serv-U 15.5.4

Advisory Details

Severity

9.1 Critical

Advisory ID

CVE-2025-40538

First Published

02/24/26

Last Published

02/24/26

Version

SolarWinds Serv-U 15.5.4

CVSS Score

CVSS:9.1AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H