Active Exploitation of SolarWinds Serv-U File Transfer Servers

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

CISA has confirmed active exploitation of CVE-2026-28318 (CVSS 7.5), an unauthenticated denial-of-service vulnerability affecting SolarWinds Serv-U file transfer servers.

Successful exploitation can cause the Serv-U service to crash, disrupting file transfer operations used by organizations to exchange sensitive business data.

Overview

There is an uncontrolled resource consumption vulnerability (CVE-2026-28318, CVSS 7.5) in SolarWinds Serv-U that may allow an unauthenticated threat actor to crash the Serv-U service.

Affected Products

- SolarWinds Serv-U 15.5.4 and earlier versions

SolarWinds Serv-U is a Managed File Transfer (MFT) and FTP server solution used on Windows and Linux systems to securely exchange files over HTTP/HTTPS, FTP, FTPS, and SFTP. Organizations often use the platform to transfer sensitive business information between employees, customers, vendors, partners, and third parties.

According to SolarWinds, a threat actor can exploit CVE-2026-28318 by sending specially crafted HTTP POST requests containing the "**Content-Encoding: deflate**" header. No authentication, privileges, or user interaction are required. CISA added the vulnerability to the KEV Catalog after confirming exploitation in the wild.

The vulnerability does not provide remote code execution or direct access to data. However, it can disrupt file transfer operations that organizations rely on to exchange business-critical information. Organizations in healthcare, financial services, government, manufacturing, legal services, retail, and managed service providers may be affected because managed file transfer platforms are often used to move sensitive or regulated data.

Aspire Protects

- **Patch** – Upgrade to SolarWinds Serv-U 15.5.4 immediately. See SolarWinds' security advisory for additional details.
- Restrict access to Serv-U servers to trusted IP addresses where possible.
- Configure web application firewalls (WAFs) to block HTTP POST requests containing the "Content-Encoding: deflate" header.
- Monitor Serv-U systems for unexpected service crashes and unusual HTTP POST request activity.
- Review internet-facing Serv-U deployments and remove unnecessary external exposure.

TTPs

Initial Access

- Exploit Public-Facing Application [T1190] – Threat actors may target internet-facing Serv-U servers with crafted requests designed to trigger the vulnerability.

Impact

- Endpoint Denial of Service [T1499] – Exploitation may cause the Serv-U service to crash and interrupt file transfer operations.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

The SolarWinds Serv-U vulnerability may impact organizations that rely on managed file transfer services to exchange sensitive or regulated information.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

SolarWinds Trust Center Security Advisories | CVE-2026-28318 | SolarWinds

CVE Record: CVE-2026-28318

CISA Adds One Known Exploited Vulnerability to Catalog | CISA