INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-05 19:19 UTC

# SolarWinds Serv-U Unauthenticated Denial-of-Service via Uncontrolled Resource Consumption (CVE-2026-28318)

**CVE VULNERABILITY** | **HIGH** | CVSS 7.5 | **CISA KEV**

| | |
|---|---|
| **SCC Item ID** | SCC-CVE-2026-0268 |
| **Type** | CVE Vulnerability |
| **CVE ID** | CVE-2026-28318 |
| **Severity** | HIGH |
| **CVSS Base Score** | 7.5 |
| **EPSS Score** | 0.0006 (20th percentile) |
| **KEV Status** | Yes — CISA Known Exploited Vulnerability (due: 2026-06-19) |
| **Affected Products** | SolarWinds Serv-U (specific version range not confirmed in available data) |
| **Published** | 2026-06-05 |
| **Discovery Source** | Cisa Kev |

## Executive Summary

A confirmed, actively exploited vulnerability in SolarWinds Serv-U file transfer software allows any unauthenticated attacker to crash the service remotely by sending a single crafted request. No credentials or insider access are required. Organizations running Serv-U for managed file transfer face potential disruption to file sharing operations and any business processes that depend on them.

## Technical Analysis

CVE-2026-28318 is an uncontrolled resource consumption flaw (CWE-400) in SolarWinds Serv-U. An unauthenticated remote attacker can crash the Serv-U service by sending a specially crafted HTTP POST request with a 'Content-Encoding: deflate' header. The attack is network-accessible, requires no authentication, and is rated CVSS 7.5 (High). MITRE ATT&CK maps to T1499 (Endpoint Denial of Service) and T1499.002 (Service Exhaustion Flood). The vulnerability is listed in the CISA Known Exploited Vulnerabilities (KEV) catalog with a remediation due date of 2026-06-19, confirming active exploitation in the wild. Customers must consult the NVD entry and SolarWinds security advisory for the complete list of affected versions before applying patches. EPSS score is 0.00062 (19.65th percentile), though KEV listing supersedes EPSS as the primary exploitation signal. No CVSS vector string was available in the source data. Verify affected versions and patch availability directly at the NVD entry (https://nvd.nist.gov/vuln/detail/CVE-2026-28318) and the CISA KEV

catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog).

## Action Checklist

1. Step 1: Containment. Immediately restrict inbound access to Serv-U service ports (typically TCP 443, 22, 21) at the perimeter firewall or load balancer to trusted IP ranges only. If Serv-U is internet-facing without access controls, take it offline or place it behind a WAF or reverse proxy until patched. Reference NIST IR-4 (Incident Handling) for containment decision authority.
2. Step 2: Detection. Query web/application server logs for POST requests containing the 'Content-Encoding: deflate' header targeting Serv-U endpoints. Look for repeated service crashes or unexpected Serv-U process restarts in Windows Event Logs (Event ID 7034: Service Control Manager, service terminated unexpectedly) and Serv-U application logs. Correlate with source IP frequency to identify scanning or exploitation attempts. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication. Apply the SolarWinds-issued patch for CVE-2026-28318 as soon as it is available. Confirm the patched version from the official SolarWinds security advisory at the SolarWinds Trust Center (https://www.solarwinds.com/trust-center/). If no patch is available yet, implement an IPS/WAF rule to block or inspect POST requests with 'Content-Encoding: deflate' to Serv-U endpoints as a temporary mitigation.
4. Step 4: Recovery. After patching, restart the Serv-U service and confirm it remains stable under normal load. Validate that file transfer operations resume successfully. Monitor Serv-U process health and service availability for 72 hours post-remediation. Review AU-3 (Content of Audit Records) to confirm logs capture service state changes for ongoing verification.
5. Step 5: Post-Incident. Review whether Serv-U was internet-exposed without compensating controls; implement network segmentation or access restrictions per CIS 4.4 (Implement and Manage a Firewall on Servers). Assess whether a vulnerability management process (CIS 7.1) would have surfaced this CVE before active exploitation. Ensure the CISA KEV catalog is part of your routine vulnerability prioritization workflow. Document this incident per NIST IR-5 (Incident Monitoring) and IR-8 (Incident Response Plan).

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate to senior IR leadership and legal/compliance if forensic review of Serv-U access logs reveals successful connections from exploitation source IPs prior to containment, if Serv-U was used to transfer data subject to HIPAA, PCI-DSS, or state breach notification law, or if the team lacks the capability to implement WAF/IPS compensating controls before a vendor patch is available given active exploitation status confirmed in the CISA KEV catalog. |
| **Recovery Notes** | After applying the SolarWinds patch for CVE-2026-28318, confirm the Serv-U service version via registry key `HKLM\SOFTWARE\RhinoSoft.com\Serv-U\Version` and validate it matches the patched release documented in the SolarWinds security advisory. Monitor Windows System Event Log for Event ID 7034 referencing Serv-U and Serv-U application logs continuously for a minimum of 72 hours to confirm the crash-on-single-request behavior is no longer reproducible. Do not restore full public internet access to Serv-U ports until the patched version is confirmed stable and firewall rules scoped to trusted IP ranges remain in place as a permanent compensating layer. |

| | |
|---|---|
| **Forensic Artifacts** | Serv-U application log (`C:\ProgramData\RhinoSoft\Serv-U\Serv-U.log`): captures service crash timestamps and client connection events; correlate crash entries against HTTP request timestamps to identify the source IP delivering the CVE-2026-28318 triggering request. \| Windows System Event Log — Event ID 7034 (Service Control Manager, source 'Serv-U'): records each unexpected Serv-U process termination caused by the uncontrolled resource consumption crash; timestamp density reveals whether exploitation was targeted or mass-scan driven. \| Windows Application Event Log — Event ID 1000 (Application Error, faulting application `Serv-U.exe`): captures the faulting module, exception code, and offset at time of crash, providing evidence of the specific memory/resource exhaustion condition triggered by the crafted request. \| Perimeter firewall or load balancer access logs for TCP 21/22/443: preserve raw connection records including source IPs, connection duration, and byte counts for sessions immediately preceding each Serv-U crash event; short-duration high-frequency connections from a single IP are characteristic of DoS probe or exploitation attempts against this CVE. \| WAF or reverse proxy HTTP access logs with full header capture: the `Content-Encoding: deflate` header in a POST request to a Serv-U endpoint is the specific exploitation indicator for CVE-2026-28318; these logs are the primary artifact for attribution and for validating whether a WAF compensating rule successfully blocked exploitation attempts. |

### Per-Action IR Details

**Step 1: Containment — Immediately restrict inbound access to Serv-U service ports (typically TCP 443, 22, 21) at the perimeter firewall or load balancer to trusted IP ranges only. If Serv-U is internet-facing without access controls, take it offline or place it behind a WAF/reverse proxy until patched. Reference NIST IR-4 (Incident Handling) for containment decision authority.**

**NIST Phase:** Containment

**Reference:** NIST 800-61r3 §3.3 — Containment Strategy

**Controls:** NIST IR-4 (Incident Handling), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

**Compensating:** On Windows hosts running Serv-U, use Windows Firewall via PowerShell to immediately restrict inbound access: `New-NetFirewallRule -DisplayName 'Block Serv-U Public' -Direction Inbound -LocalPort 21,22,443 -Protocol TCP -Action Block`; then add a second rule scoped to your trusted IP range: `New-NetFirewallRule -DisplayName 'Allow Serv-U Trusted' -Direction Inbound -LocalPort 21,22,443 -Protocol TCP -RemoteAddress -Action Allow`. For Linux-hosted deployments, equivalent iptables rules achieve the same result. A 2-person team can execute this without enterprise tooling in under 10 minutes.

**Evidence:** Before restricting access, capture a full netstat snapshot to document active connections to Serv-U ports at time of containment: `netstat -ano | findstr ':21 :22 :443'` on Windows. Export Windows Firewall connection logs (`%SystemRoot%\System32\LogFiles\Firewall\pfirewall.log`) covering the 24 hours prior to containment. These preserve attacker source IPs that may be lost once traffic is blocked and connection state clears.

**Step 2: Detection — Query web/application server logs for POST requests containing the 'Content-Encoding: deflate' header targeting Serv-U endpoints. Look for repeated service crashes or unexpected Serv-U process restarts in Windows Event Logs (Event ID 7034: Service Control Manager — service terminated unexpectedly) and Serv-U application logs. Correlate with source IP frequency to identify scanning or exploitation attempts. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2 — Detection and Analysis

**Controls:** NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-3 (Content Of Audit Records), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

**Compensating:** Without a SIEM, run this PowerShell command on the Serv-U Windows host to extract Event ID 7034 occurrences referencing the Serv-U service: `Get-WinEvent -LogName System | Where-Object {$_.Id -eq 7034 -and $_.Message -like '*Serv-U*'} | Select-Object TimeCreated, Message | Export-Csv servu_crashes.csv`. For HTTP log analysis, use `findstr /i 'deflate' ` against Serv-U's access log directory (default: `C:\ProgramData\RhinoSoft\Serv-U\Serv-U.log` or configured log path). Correlate crash timestamps against HTTP request timestamps manually to identify the triggering source IP.

**Evidence:** Preserve the following before any log rotation occurs: Serv-U application log (default path `C:\ProgramData\RhinoSoft\Serv-U\Serv-U.log`) showing service start/stop events correlated with crash times; Windows System Event Log filtered for Event ID 7034 with source 'Service Control Manager' referencing 'Serv-U'; Windows Application Event Log for any Serv-U process fault entries (Event ID 1000 — Application Error, faulting application `Serv-U.exe`); and any WAF or load balancer access logs capturing the raw HTTP headers, specifically the `Content-Encoding: deflate` header pattern in requests to Serv-U listener ports.

**Step 3: Eradication — Apply the SolarWinds-issued patch for CVE-2026-28318 as soon as it is available. Confirm the patched version from the official SolarWinds security advisory at https://www.solarwinds.com/trust-center/security-advisories (note: verify this URL resolves to the current advisory — URL not confirmed in verified reference list). If no patch is available yet, implement an IPS/WAF rule to block or inspect POST requests with 'Content-Encoding: deflate' to Serv-U endpoints as a temporary mitigation.**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication

**Controls:** NIST SI-1 (Policy And Procedures), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management)

**Compensating:** If a WAF is unavailable, deploy an IPS rule using Snort or Suricata (both free) targeting POST requests to Serv-U listener ports containing the `Content-Encoding: deflate` header — example Suricata rule: `alert http any any -> $SERVU_HOST [21,22,443] (msg:"CVE-2026-28318 Serv-U DoS attempt"; http.method; content:"POST"; http.header; content:"Content-Encoding: deflate"; sid:2026283180; rev:1;)`. Alternatively, on the Serv-U Windows host, create a Windows Firewall rule blocking all POST-bearing traffic is not header-inspectable at that layer — escalate to a network choke point using Wireshark in capture mode to at minimum alert on the pattern while the patch is pending.

**Evidence:** Before applying the patch, record the currently installed Serv-U version by checking `HKLM\SOFTWARE\RhinoSoft.com\Serv-U\Version` in the Windows registry or via `wmic product where name='Serv-U' get version`. Capture a hash of the Serv-U executable (`Get-FileHash 'C:\Program Files\RhinoSoft\Serv-U\Serv-U.exe' -Algorithm SHA256`) pre- and post-patch to confirm the binary was replaced. Retain these pre-patch artifacts for change management records and to verify the vulnerable version is no longer present.

**Step 4: Recovery — After patching, restart the Serv-U service and confirm it remains stable under normal load. Validate that file transfer operations resume successfully. Monitor Serv-U process health and service availability for 72 hours post-remediation. Review AU-3 (Content of Audit Records) to confirm logs capture service state changes for ongoing verification.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** NIST AU-3 (Content Of Audit Records), NIST AU-8 (Time Stamps), NIST CP-10 (System Recovery And Reconstitution)

**Compensating:** Use the free Sysinternals Process Monitor (`procmon.exe`) during the first 30 minutes after Serv-U restart to confirm the service process (`Serv-U.exe`) remains stable and does not exhibit crash/restart cycles. Set a scheduled task to poll Serv-U service state every 5 minutes via PowerShell: `while ($true) { $s = Get-Service 'Serv-U'; Write-Output "$(Get-Date) — $($s.Status)" | Tee-Object -Append servu_health.log; Start-Sleep 300 }`. Alert on any status other than 'Running'. For a 2-person team, one analyst monitors this output while the second validates file transfer functionality with a test transfer to/from a controlled endpoint.

**Evidence:** After the Serv-U service restart post-patch, capture Windows System Event Log entries for Event ID 7036 (Service Control Manager — service entered running state) and Event ID 7034 (unexpected termination) to confirm no post-patch crash occurs. Retain Serv-U application log entries for the 72-hour monitoring window as documented evidence of service stability. Record the patched binary hash (`Get-FileHash 'C:\Program Files\RhinoSoft\Serv-U\Serv-U.exe' -Algorithm SHA256`) to confirm it differs from the pre-patch value captured during eradication.

**Step 5: Post-Incident — Review whether Serv-U was internet-exposed without compensating controls; implement network segmentation or access restrictions per CIS 4.4 (Implement and Manage a Firewall on Servers). Assess whether a vulnerability management process (CIS 7.1) would have surfaced this CVE before active exploitation. Ensure the CISA KEV catalog is part of your routine vulnerability prioritization workflow. Document this incident per NIST IR-5 (Incident Monitoring) and IR-8 (Incident Response Plan).**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §4 — Post-Incident Activity

**Controls:** NIST IR-5 (Incident Monitoring), NIST IR-8 (Incident Response Plan), NIST AU-11 (Audit Record Retention), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

**Compensating:** To operationalize CISA KEV monitoring without enterprise tooling, use a free cron job or scheduled task to pull the CISA KEV JSON feed daily (`https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json`) and diff it against your asset inventory: `curl -s https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json | python3 -c "import sys,json; [print(v['cveID'],v['vendorProject'],v['product']) for v in json.load(sys.stdin)['vulnerabilities'] if 'SolarWinds' in v['vendorProject']]"`. This surfaces newly added SolarWinds entries including Serv-U CVEs the day CISA catalogs them. Note: verify the KEV feed URL resolves correctly — this is a well-known CISA resource but confirm before scripting.

**Evidence:** Retain the complete incident record including: pre-containment netstat capture, Serv-U crash event log exports (Event IDs 7034 and 1000), HTTP access log excerpts showing `Content-Encoding: deflate` requests, pre- and post-patch binary hashes, and the 72-hour post-recovery health log. These artifacts satisfy NIST AU-11 (Audit Record Retention) retention requirements and provide evidence for any regulatory notification assessment if Serv-U was used to transfer PII or PHI.

## Detection Guidance

Primary detection signal: search web access logs and Serv-U application logs for HTTP POST requests carrying the 'Content-Encoding: deflate' header, particularly at high frequency from a single source IP or across short time windows. Secondary signal: monitor the Windows Service Control Manager for Event ID 7034 (service terminated unexpectedly) referencing the Serv-U service process. A pattern of repeated service crashes following POST request bursts is a strong indicator of active exploitation. If a SIEM is in use, build a correlation rule combining Serv-U process restarts with inbound POST traffic anomalies. If network IDS/IPS is deployed, create a signature matching POST requests with 'Content-Encoding: deflate' destined for Serv-U listener ports. Baseline: normal Serv-U operations should not produce repeated service crashes. Any unplanned service termination warrants investigation. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and AU-12 (Audit Record Generation) for logging requirements, and CIS 8.2 (Collect Audit Logs) for baseline log collection coverage.

## Framework Mappings

**MITRE-ATTACK**

- **T1499** — Endpoint Denial of Service
- **T1499.002** — Service Exhaustion Flood

### NIST-800-53R5

- **SC-5** — Denial-of-Service Protection
- **IR-5** — Incident Monitoring

### CIS-V8

- **13.8** — Deploy a Network Intrusion Prevention Solution

### ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

### NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1499 | Endpoint Denial of Service | Impact |
| T1499.002 | Service Exhaustion Flood | Impact |

## Sources

| Source | URL | Tier |
|---|---|---|
| **cisa_kev** | https://www.cisa.gov/known-exploited-vulnerabilities-catalog | T1 |
| **CVE-2026-28318 Detail - NVD** | https://nvd.nist.gov/vuln/detail/CVE-2026-28318 | T1 |
| **CVE-2026-28318 - SolarWinds Serv-U Unauthenticated Denial of ...** | https://cvefeed.io/vuln/detail/CVE-2026-28318 | T3 |
| **CVE-2026-28318 \| Tenable®** | https://www.tenable.com/cve/CVE-2026-28318 | T3 |
| **Elasticsearch 8.19.8, 9.1.8 Security Update (ESA-2026-18)** | https://discuss.elastic.co/t/elasticsearch-8-19-8-9-1-8-security-up... | T3 |

Generated 2026-06-05 19:19 UTC by TJS Security Command Center