مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Security Updates-SolarWinds Serv-U

Tracking #:432319321

Date:22-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed SolarWinds has released security updates to address 16 security vulnerabilities, including 15 Critical vulnerabilities SolarWinds Serv-U Managed File Transfer (MFT) and Serv-U Gateway.

TECHNICAL DETAILS:

SolarWinds has released Serv-U 2026.3 to address 16 security vulnerabilities, including 15 Critical vulnerabilities (CVSS 9.1) and one Medium severity Stored Cross-Site Scripting (XSS) vulnerability (CVSS 6.2) affecting SolarWinds Serv-U Managed File Transfer (MFT) and Serv-U Gateway. The critical vulnerabilities include Insecure Direct Object Reference (IDOR), Privilege Escalation, Broken Access Control, and Remote Code Execution (RCE) flaws that could allow authenticated attackers to escalate privileges, compromise administrator accounts, execute arbitrary code as the root user (primarily on Linux), perform account takeover, hijack SMTP functionality, and gain unauthorized access to sensitive files.

Vulnerability Details:

- **CVE-2026-28302 – IDOR Privilege Escalation and Root Remote Code Execution**
  - **CVSS:** 9.1 (Critical)
- **CVE-2026-28304 – Remote Code Execution as Root**
  - **CVSS:** 9.1 (Critical)
- **CVE-2026-28305 – IDOR Leading to Root Remote Code Execution**
  - **CVSS:** 9.1 (Critical)
- **CVE-2026-28306 – Domain Administrator Privilege Escalation**
  - **CVSS:** 9.1 (Critical)
- **CVE-2026-28307 – Domain User Group Privilege Escalation**
  - **CVSS:** 9.1 (Critical)
- **CVE-2026-28308 – IDOR Leading to Remote Code Execution**
  - **CVSS:** 9.1 (Critical)
- **CVE-2026-28309 – Broken Access Control Allowing System Administrator Creation**
  - **CVSS:** 9.1 (Critical)
- **CVE-2026-28310 – User Type Privilege Escalation**
  - **CVSS:** 9.1 (Critical)
- **CVE-2026-28311 – Application Behavior Manipulation Leading to Remote Code Execution**
  - **CVSS:** 9.1 (Critical)
- **CVE-2026-28312 – Group Privilege Escalation with Root Code Execution**
  - **CVSS:** 9.1 (Critical)
- **CVE-2026-28313 – IDOR Leading to SMTP Hijacking and Account Takeover**
  - **CVSS:** 9.1 (Critical)
- **CVE-2026-28314 – IDOR Account Takeover**
  - **CVSS:** 9.1 (Critical)
- **CVE-2026-28315 – Stored Cross-Site Scripting (XSS)**
  - **CVSS:** 6.2 (Medium)
- **CVE-2026-28316 – IDOR Privilege Escalation with Root Command Execution**
  - **CVSS:** 9.1 (Critical)
- **CVE-2026-28317 – IDOR Privilege Escalation**

- **CVSS:** 9.1 (Critical)

- **CVE-2026-28321 – Broken Access Control Leading to Arbitrary File Read/Write and Root Code Execution**
  - **CVSS:** 9.1 (Critical)

Affected Products:

- SolarWinds Serv-U Managed File Transfer
- SolarWinds Serv-U Gateway

Affected Versions

- Serv-U 15.5.4 HF1 and earlier

Fixed Version

- Serv-U 2026.3

RECOMMENDATIONS:

Immediate Actions:

- Immediately upgrade all Serv-U installations to fixed versions.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_2026-3_release_notes.htm