Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2026-0265

## Kwetsbaarheden verholpen in SolarWinds Serv-U

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 27-07-2026

**TLP:WHITE**

**Toegestane verspreiding van TLP:WHITE**
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

## Feiten

SolarWinds heeft meerdere kwetsbaarheden verholpen in Serv-U.

## Duiding

De kwetsbaarheden in SolarWinds Serv-U betreffen voornamelijk insecure direct object reference (IDOR) en broken access control. Deze maken het mogelijk voor aanvallers met bepaalde privileges, zoals domain administrator of group administrator toegang, om privileges te escaleren naar system administrator of root-niveau. Hierdoor kunnen zij op afstand willekeurige code uitvoeren en systeembeheerrechten verkrijgen.

Sommige kwetsbaarheden maken het ook mogelijk om SMTP-sessies te kapen, accounts over te nemen, of persistent cross-site scripting (XSS) uit te voeren die sessies van beheerders kan compromitteren. De impact van deze kwetsbaarheden is op Windows-omgevingen doorgaans minder groot dan op andere platformen. Exploitatie vereist meestal dat de aanvaller al beschikt over geauthenticeerde toegang met hoge privileges, zoals domain administrator rechten.

De verholpen kwetsbaarheden betreffen zoals gezegd overwegend kwetsbaarheden die kunnen worden misbruikt in zo genaamde 'Evil Admin'-scenario's. Dit soort kwetsbaarheden zijn doorgaans niet eenvoudig te misbruiken door ongeathenticeerde kwaadwillenden op afstand. Echter zijn er in deze updates dermate veel verholpen dat het aan te raden is om, naast het inzetten van de updates, te controleren hoe de rechtenstructuur is geïmplementeerd. Dit geldt voornamelijk voor onderdelen die publiek toegankelijk zijn.

## Oplossingen

SolarWinds heeft updates uitgebracht om de kwetsbaarheden in Serv-U te verhelpen. Zie bijgevoegde referenties voor meer informatie.

## Referenties

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

## Kwetsbaarheden

| CVE | CVSS Score |
| --- | --- |
| CVE-2026-28302 | 9.1 CRITICAL |
| CVE-2026-28304 | 9.1 CRITICAL |

| | |
|---|---|
| CVE-2026-28305 | 9.1 CRITICAL |
| CVE-2026-28306 | 9.1 CRITICAL |
| CVE-2026-28307 | 9.1 CRITICAL |
| CVE-2026-28308 | 9.1 CRITICAL |
| CVE-2026-28309 | 9.1 CRITICAL |
| CVE-2026-28310 | 9.1 CRITICAL |
| CVE-2026-28312 | 9.1 CRITICAL |
| CVE-2026-28313 | 9.1 CRITICAL |
| CVE-2026-28314 | 9.1 CRITICAL |
| CVE-2026-28315 | 6.2 MEDIUM |
| CVE-2026-28316 | 9.1 CRITICAL |
| CVE-2026-28317 | 9.1 CRITICAL |
| CVE-2026-28321 | 9.1 CRITICAL |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
| CWE-284 | Improper Access Control |
| CWE-285 | Improper Authorization |
| CWE-639 | Authorization Bypass Through User-Controlled Key |
| CWE-862 | Missing Authorization |

## Getroffen producten

| SolarWinds |
| --- |
| Serv-<br>U |

## Disclaimer