



# NCSC-2026-0042

## Kwetsbaarheden verholpen in SolarWinds Web Help Desk

NCSC Advisory

**PRIORITEIT: HOOG**

Gepubliceerd op: 02-02-2026

Revisie: 1.0.1

**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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Update Revisie 1

Er is Proof-of-Concept-code verschenen die de kwetsbaarheid met kenmerk CVE-2025-40554 kan aantonen. Met name installaties die publiek benaderbaar zijn lopen hierdoor verhoogd risico.

## Feiten

SolarWinds heeft kwetsbaarheden verholpen in SolarWinds Web Help Desk.

## Duiding

De kwetsbaarheden omvatten onder andere de mogelijkheid voor ongeauthenticeerde aanvallers om toegang te krijgen tot beperkte functionaliteiten binnen het systeem, het gebruik van hardcoded credentials die ongeautoriseerde toegang tot administratieve functies kunnen verlenen, en kwetsbaarheden gerelateerd aan onbetrouwbare data-deserialisatie die mogelijk op afstand code-executie kunnen mogelijk maken. Daarnaast is er een kwetsbaarheid die het mogelijk maakt om authenticatiemechanismen te omzeilen, wat kan leiden tot ongeautoriseerde toegang en de mogelijkheid om specifieke acties binnen het systeem uit te voeren.

*Update:* Voor de kwetsbaarheid met kenmerk CVE-2025-40554 is Proof-of-Concept-code (PoC) verschenen. De werking van de PoC is niet door het NCSC gevalideerd en er wordt op dit moment (nog) geen grootschalig misbruik waargenomen, maar het NCSC verwacht een toename in scan- en misbruikverkeer, met name bij systemen die publiek toegankelijk zijn.

## Oplossingen

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

## Referenties

- <https://www.solarwinds.com/trust-center/security-advisories>
- <https://www.solarwinds.com/trust-center/security-advisories/CVE-2025-40536>
- <https://www.solarwinds.com/trust-center/security-advisories/CVE-2025-40537>
- <https://www.solarwinds.com/trust-center/security-advisories/CVE-2025-40551>
- <https://www.solarwinds.com/trust-center/security-advisories/CVE-2025-40553>
- <https://www.solarwinds.com/trust-center/security-advisories/CVE-2025-40554>

Kwetsbaarheden

| CVE              | CVSS Score |
|------------------|------------|
| > CVE-2025-40536 | 6.3 MEDIUM |
| > CVE-2025-40537 | 2.3 LOW    |
| > CVE-2025-40551 | 6.9 MEDIUM |
| > CVE-2025-40553 | 6.9 MEDIUM |
| > CVE-2025-40554 | 6.9 MEDIUM |

CWE's

| CWE        | Beschrijving                      |
|------------|-----------------------------------|
| > CWE-502  | Deserialization of Untrusted Data |
| > CWE-693  | Protection Mechanism Failure      |
| > CWE-798  | Use of Hard-coded Credentials     |
| > CWE-1390 | Weak Authentication               |

Getroffen producten

|                   |
|-------------------|
| <b>SolarWinds</b> |
| Web Help<br>Desk  |

## Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy or incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.