

# CVE-2024-28986

## SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability

CISA KEV since Aug 15, 2024

Actively exploited

SolarWinds Web Help Desk was found to be susceptible to a Java Deserialization Remote Code Execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. While it was reported as an unauthenticated vulnerability, SolarWinds has been unable to reproduce it without authentication after thorough testing. However, out of an abundance of caution, we recommend all Web Help Desk customers apply the patch, which is now available.

|                                                                |                                                          |                                                                   |                                                                                           |
|----------------------------------------------------------------|----------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <p>EVRS</p> <p><b>83</b>/100</p> <p><b>Urgent</b> priority</p> | <p>CVSS V3.1</p> <p><b>9.8</b></p> <p>Critical · NVD</p> | <p>EPSS</p> <p><b>0.846</b></p> <p>99.71st percentile · FIRST</p> | <p>CISA DEADLINE</p> <p><b>Sep 5, 2024</b></p> <p>KEV since 2024 · listed over a year</p> |
|----------------------------------------------------------------|----------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                     |                                          |                                                                |                                            |
|-----------------------------------------------------|------------------------------------------|----------------------------------------------------------------|--------------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b> | Listed in the catalog                    | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild         |
| <input type="checkbox"/> <b>Ransomware</b>          | No known ransomware campaign association | <input type="checkbox"/> <b>KEV recency</b>                    | On the CISA KEV catalog for over two years |
| <input checked="" type="checkbox"/> <b>EPSS</b>     | 0.846 probability                        | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable              |
| <input checked="" type="checkbox"/> <b>CVSS</b>     | Base score 9.8                           | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                        |

### Remediation

**Patch This Cycle** Patch or fixed version identified

**CISA required action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

### Affected and fixed versions

| PACKAGE       | AFFECTED           | FIXED IN     | SOURCE |
|---------------|--------------------|--------------|--------|
| web help desk | ≤ 12.8.2<br>12.8.3 | after 12.8.2 | NVD    |

### Sources

|                        |                                                                                                                                                     |                            |                                                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Vendor guidance</b> | <a href="https://github.com/advisories/GHSA-g536-h677-2w32">github.com/advisories/GHSA-g536-h677-2w32</a>                                           | <b>Additional guidance</b> | <a href="https://support.solarwinds.com/SuccessCenter/s/article/WHD-12-8-3-Hotfix-1">support.solarwinds.com/SuccessCenter/s/article/WHD-12-8-3-Hotfix-1</a> |
| <b>solarwinds.com</b>  | <a href="https://solarwinds.com/trust-center/security-advisories/cve-2024-28986">solarwinds.com/trust-center/security-advisories/cve-2024-28986</a> | <b>NVD</b>                 | <a href="https://nvd.nist.gov/vuln/detail/CVE-2024-28986">nvd.nist.gov/vuln/detail/CVE-2024-28986</a>                                                       |
| <b>CISA KEV</b>        | <a href="https://cisa.gov/known-exploited-vulnerabilities-catalog">cisa.gov/known-exploited-vulnerabilities-catalog</a>                             | <b>ENISA EUVD</b>          | <a href="https://euvd.enisa.europa.eu/vulnerability/EUVD-2024-26048">euvd.enisa.europa.eu/vulnerability/EUVD-2024-26048</a>                                 |
| <b>Current data</b>    | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2024-28986">evulnable.com/vulnerability-management/cve/CVE-2024-28986</a>           |                            |                                                                                                                                                             |

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.