

CVE-2025-40551

SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability

CISA KEV since Feb 3, 2026

Actively exploited

Public exploit module (Metasploit)

SolarWinds Web Help Desk was found to be susceptible to an untrusted data deserialization vulnerability that could lead to remote code execution, which would allow an attacker to run commands on the host machine. This could be exploited without authentication.

EVRS 86/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.842 99.7th percentile · FIRST	CISA DEADLINE Feb 6, 2026 CISA federal deadline · Overdue by 8 months
--	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.842 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, 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	< 2026.1	2026.1	NVD

Sources

Vendor guidance github.com/advisories/GHSA-7qrj-j83p-3vqg

Additional guidance solarwinds.com/trust-center/security-advisories/CVE-2025-40551

solarwinds.com solarwinds.com/trust-center/security-advisories/cve-2025-40551

NVD nvd.nist.gov/vuln/detail/CVE-2025-40551

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-206426

Current data evulnable.com/vulnerability-management/cve/CVE-2025-40551

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