

CVE-2025-40536

SolarWinds Web Help Desk Security Control Bypass Vulnerability

CISA KEV since Feb 12, 2026

Actively exploited

Public exploit module (Metasploit)

SolarWinds Web Help Desk was found to be susceptible to a security control bypass vulnerability that if exploited, could allow an unauthenticated attacker to gain access to certain restricted functionality.

EVRS 83/100 Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.736 99.47th percentile · FIRST	CISA DEADLINE Feb 15, 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	0.736 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle 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-m83h-48rr-jcrh	Additional guidance	solarwinds.com/trust-center/security-advisories/CVE-2025-40536
documentation.solarwinds.com	documentation.solarwinds.com/en/success_center/whd/content/release_notes/whd_2026-1_release_notes.htm	NVD	nvd.nist.gov/vuln/detail/CVE-2025-40536
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-206418
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-40536		

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