

CVE-2024-28987

SolarWinds Web Help Desk Hardcoded Credential Vulnerability

Exigent

CISA KEV since Oct 15, 2024

Actively exploited

Public exploit module (Metasploit)

The SolarWinds Web Help Desk (WHD) software is affected by a hardcoded credential vulnerability, allowing remote unauthenticated user to access internal functionality and modify data.

EVRS 85 /100 Immediate priority	CVSS V3.1 9.1 Critical · NVD	EPSS 0.933 99.84th percentile · FIRST	CISA DEADLINE Nov 5, 2024 KEV since 2024 · listed over a year
--	--	---	---

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	On the CISA KEV catalog for over two years
☒ EPSS	0.933 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent 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	< 12.8.3 12.8.3	12.8.3	NVD

Sources

Vendor guidance github.com/advisories/GHSA-4jq7-4qmf-m333

Additional guidance solarwinds.com/trust-center/security-advisories/cve-2024-28987

NVD nvd.nist.gov/vuln/detail/CVE-2024-28987

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2024-26049

Current data evulnable.com/vulnerability-management/cve/CVE-2024-28987

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