CYBER ADVISORY

Wednesday, January 28, 2026 **CAL-CSIC-202601-A-013**

Multiple Vulnerabilities in SolarWinds Web Help Desk

Unauthorized Access | Authentication Bypass | Remote Code Execution | Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has identified multiple high and critical vulnerabilities in SolarWinds Web Help Desk that could lead to unauthorized access, authentication bypass, and unauthenticated remote code execution (RCE). These include CVE-2025-40536, security control bypass, CVE-2025-40537, hardcoded credentials, and a set of critical vulnerabilities: CVE-2025-40551, CVE-2025-40552, CVE-2025-40553, and CVE-2025-40554 all of which are rated as CVSS 9.8 in CVSS 3.1 affecting authentication and deserialization controls. Collectively, these flaws lower the barrier to compromise and significantly elevate risk for affected deployments.

SolarWinds Web Help Desk (WHD) is a widely deployed IT service management and ticketing platform. WHD plays an important role in how organizations manage support requests, track IT assets, and deliver effective service. A compromise of this application will severely impact affected organizations[1].

Analyst Comment: *Due to the nature of the vulnerabilities, automated scanning and exploit attempts are highly likely to occur on exposed instances. Although there are no widespread confirmed active exploit reports as of this advisory, the ease of exploitation and cumulative severity strongly indicate that threat actors could rapidly target vulnerable systems. Coupled with the fact Solar Winds products have traditionally been seen as a prime target[2], it further highlights the importance of ensuring WHD is up to date.*

The Cal-CSIC recommends immediately updating affected assets to *WHD 2026.1 or later*. For further information on applying the vendor's security patch and for any frequently asked questions, please use this link.

https://documentation.solarwinds.com/en/success_center/whd/content/helpdeskupgradetolatestversion.htm

SolarWinds CVEs

CVE-ID	Severity	Description
CVE-2025-40536	8.1 High	Security control bypass vulnerability that could allow an unauthenticated attacker to gain access to certain restricted functionality.
CVE-2025-40537	7.5 High	Hardcoded credentials vulnerability that could allow access to administrative functions.
CVE-2025-40551	9.8 Critical	Untrusted data deserialization vulnerability that could lead to remote code execution which would allow an attacker to run commands on the host machine.
CVE-2025-40552	9.8 Critical	Authentication bypass vulnerability that could allow a malicious actor to execute actions and methods that should be protected by authentication.
CVE-2025-40553	9.8 Critical	Untrusted data deserialization vulnerability that could lead to remote code execution which would allow an attacker to run commands on the host machine.
CVE-2025-40554	9.8 Critical	Authentication bypass vulnerability that could allow an attacker to invoke specific actions within Web Help Desk.

References

[1]Solar Winds "WHD 2026.1 release notes"; https://documentation.solarwinds.com/en/success_center/whd/content/release_notes/whd_2026-1_release_notes.htm#link4; accessed 28 January 2026

[2] Fortinet "Solar Winds Cyber Attack"; https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack; accessed 28 January 2026