SolarWinds Web Help Desk Deserialization of Untrusted Data Remote Code Execution Vulnerability (CVE-2025- 40551)

Advisory Details

Severity

9.8 Critical

Advisory ID

CVE-2025-40551

First Published

01/28/2026

Last Published

02/06/2026

Fixed Version

SolarWinds Web Help Desk 2026.1

CVSS Score

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

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.

CVE-2025-40551 is now included in the CISA Known Exploited Vulnerabilities (KEV) catalog.

Indicators of Compromise:

1. Calls to an OAST server found in WHD application logs (these can be found in “\WebHelpDesk\log\whd_yyyy-mm-dd.txt”).
2. Requests sent to the WHD server for the following URLs with keywords: “bogus”, “badparam=/ajax/…“ (these can be found in “\WebHelpDesk\logs\whd_access_log_yyyy-mm-dd.txt”).
3. More indicators of compromise can be found in Horizon3.ai's article on CVE-2025-40551

Suspicious IPs found:

- 178.128.210.172
- 137.184.229.230

Affected Products

- SolarWinds Web Help Desk 12.8.8 HF1 and all previous versions

Fixed Software Release

- SolarWinds Web Help Desk 2026.1

Acknowledgments

- Jimi Sebree working with Horizon3.ai