Security Advisory 2024-081

SolarWinds Web Help Desk Critical Remote Code Execution Vulnerability

August 16, 2024 — v1.0

TLP:CLEAR

History:

- *16/08/2024 — v1.0 – Initial publication*

Summary

On August 14, 2024, SolarWinds disclosed a critical remote code execution (RCE) vulnerability, **CVE-2024-28986**, affecting all versions of their Web Help Desk (WHD) software [1]. The vulnerability, caused by a Java deserialization flaw, allows attackers to execute arbitrary commands on the affected system. The vulnerability has a CVSS score of 9.8.

Technical Details

CVE-2024-28986 is a Java deserialization vulnerability that allows attackers to execute remote commands on the vulnerable system. Initially reported as an unauthenticated exploit, it was later confirmed to require authentication for exploitation [1].

Affected Products

- All versions of SolarWinds Web Help Desk prior to 12.8.3 with hotfix applied.

Recommendations

CERT-EU strongly recommends updating to the latest version (12.8.3) and applying the provided hotfix immediately. Additionally, create backup copies of original files before applying the patch.

References

[1] https://www.bleepingcomputer.com/news/security/solarwinds-fixes-critical-rce-bug-affecting-all-web-help-desk-versions/