SolarWinds Observability Self-Hosted Deserialization of Untrusted Data Local Privilege Escalation Vulnerability (CVE-2025-26397)

Advisory Details

Severity

7.8 High

Advisory ID

CVE-2025-26397

First Published
07/24/2025

Fixed Version
SWOSH 2025.2.1

CVSS Score

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

SolarWinds Observability Self-Hosted is susceptible to Deserialization of Untrusted Data Local Privilege Escalation vulnerability. An attacker with low privileges can escalate privileges to run malicious files copied to a permission-protected folder. This vulnerability requires authentication from a low-level account and local access to the host server.

Affected Products

- SWOSH 2025.2 and prior

Fixed Software Release

- SWOSH 2025.2.1

Acknowledgments

- ccc working with the Trend Micro Zero Day Initiative