

SolarWinds ARM Deserialization of Untrusted Data Remote Code Execution Vulnerability (CVE-2024-28075)

Summary

The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution.

We thank Trend Micro Zero Day Initiative (ZDI) for its ongoing partnership in coordinating with SolarWinds on responsible disclosure of this and other potential vulnerabilities.

Affected Products

- SolarWinds ARM 2023.2.3 and prior versions

Fixed Software Release

- [SolarWinds ARM 2023.2.4](#)

Acknowledgments

- Piotr Bazydło (@chudypb) of Trend Micro Zero Day Initiative

Advisory Details

Severity

9.0 Critical

Advisory ID

[CVE-2024-28075](#)

First Published

05/09/2024

Last Published

05/09/2024

Fixed Version

[SolarWinds ARM 2023.2.4](#)

CVSS Score

[CVSS:9.0/AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H](#)