SolarWinds Access Rights Manager (ARM) Deserialization of Untrusted Data Remote Code Execution Vulnerability (CVE-2023-40057)

Advisory Details

Severity
9.0 Critical

Advisory ID
CVE-2023-40057

First Published
02/06/2024

Last Updated
02/06/2024

Fixed Version
SolarWinds Access Rights Manager (ARM) 2023.2.3

CVSS Score
CVSS:9.0/AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Security Advisory Summary

The SolarWinds Access Rights Manager was found to be susceptible to a Remote Code Execution Vulnerability. If exploited, this vulnerability allows an authenticated user to abuse a 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 Access Rights Manager (ARM) 2023.2.2 and prior versions

Fixed Software Release

- SolarWinds Access Rights Manager (ARM) 2023.2.3

Acknowledgments

- Anonymous working with Trend Micro Zero Day Initiative