SolarWinds Access Rights Manager (ARM) UserScriptHumster Exposed Dangerous Method Remote Command Execution Vulnerability (CVE-2024-23470)

Advisory Details

Severity
9.6 Critical

Advisory ID
CVE-2024-23470

First Published
7/17/2024

Fixed Version
SolarWinds Access Rights Manager (ARM) 2024.3

CVSS Score
CVSS:9.6AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Summary

The SolarWinds Access Rights Manager was found to be susceptible to a pre-authentication remote code execution vulnerability. If exploited, this vulnerability allows an unauthenticated user to run commands and executables.

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) 2023.2.4 and prior versions

Fixed Software Release

- SolarWinds Access Rights Manager (ARM) 2024.3

Acknowledgments

- Anonymous working with Trend Micro Zero Day Initiative