

SolarWinds Access Rights Manager (ARM) ChangeHumster Exposed Dangerous Method Authentication Bypass Vulnerability (CVE-2024-23465)

Summary

The SolarWinds Access Rights Manager was found to be susceptible to an authentication bypass vulnerability. This vulnerability allows an unauthenticated user to gain domain admin access within the Active Directory environment.

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

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

Advisory Details

Severity

8.3 High

Advisory ID

[CVE-2024-23465](#)

First Published

7/17/2024

Fixed Version

[SolarWinds Access Rights Manager \(ARM\) 2024.3](#)

CVSS Score

[CVSS:8.3/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H](#)