SolarWinds Access Rights Manager (ARM) Hardcoded Credentials Authentication Bypass Vulnerability (CVE-2024-28990)

Advisory Details

Severity
6.3 Medium

Advisory ID
CVE-2024-28990

First Published
9/12/2024

Fixed Version
Access Rights Manager (ARM) 2024.3.1 SR

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

Summary

SolarWinds Access Rights Manager (ARM) was found to contain a hard-coded credential authentication bypass vulnerability. If exploited, this vulnerability would allow access to the RabbitMQ management console.

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 2024.3 and prior versions

Fixed Software Release

- Access Rights Manager (ARM) 2024.3.1 SR

Acknowledgments

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