Security Advisory 2024-097

Vulnerabilities in SolarWinds Access Rights Manager

2024-09-16 — v1.0

TLP:CLEAR

History:

- *16/09/2024 — v1.0 – Initial publication*

Summary

On September 12, 2024, Solarwinds released several advisories addressing two critical vulnerabilities in SolarWinds Access Rights Manager (ARM). These vulnerabilities, if exploited, could lead to authenticated remote code execution, and authentication bypass [1][2].

Technical Details

The vulnerability **CVE-2024-28990**, with a CVSS Score of 6.3, is a hard-coded credential authentication bypass flaw. If exploited, this vulnerability would allow access to the RabbitMQ management console.

The vulnerability **CVE-2024-28991**, with a CVSS Score of 9.0, is a deserialisation of untrusted data flaw that, if exploited, could lead to remote code execution on the affected server.

Affected Products

These vulnerabilities affect SolarWinds Access Rights Manager (ARM) before the version 2024.3.1 (fixed release).

Recommendations

CERT-EU strongly recommends updating software installations to a fixed version [1][2].

References

[1] https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28990

[2] https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28991