CERT-EU

Security Advisory 2024-071

Critical Vulnerabilities in SolarWinds Access Rights Manager

July 19, 2024 — v1.0

TLP:CLEAR

History:

- *19/07/2024 — v1.0 – Initial publication*

Summary

On July 18, 2024, SolarWinds issued an advisory addressing multiple critical vulnerabilities in its Access Rights Manager (ARM) software [1,2]. These vulnerabilities could lead to remote code execution, arbitrary file deletion and sensitive information leakage.

It is recommended updating affected systems immediately.

Technical Details

The vulnerabilities **CVE-2024-23469**, **CVE-2024-23466**, **CVE-2024-23467**, **CVE-2024-28074**, **CVE-2024-23471**, and **CVE-2024-23470**, all with a CVSS score of 9.6, could lead to remote code execution if exploited. They are due to various critical flaws.

The vulnerabilities **CVE-2024-23475**, and **CVE-2024-23472**, both with a CVSS score of 9.6, are directory traversal and sensitive information disclosure flaws.

The vulnerability **CVE-2024-23465**, with a CVSS score of 8.3, is an authentication bypass vulnerability.

Affected Products

- SolarWinds Access Rights Manager versions prior to 2024.3.

Recommendations

CERT-EU recommends updating affected devices to the latest version of SolarWinds Access Rights Manager as soon as possible.

References

[1] https://www.bleepingcomputer.com/news/security/solarwinds-fixes-8-critical-bugs-in-access-rights-audit-software/

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