July 18, 2024

Overall Rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of SolarWinds published security advisories to address critical vulnerabilities in the following product:

- SolarWinds Access Rights Manager (ARM) – version 2023.2.4 and prior

Technical Details

It was discovered that a previous vulnerability was not completely fixed with SolarWinds Access Rights Manager. While some controls were implemented the researcher was able to bypass these and use a different method to exploit the vulnerability.

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.

This vulnerability is rated as a **CRITICAL** risk. Software updates exist to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at vulnerabilityandriskmanagement@gov.bc.ca

References

- CVE-2024-23471 CVE-2024-23469 CVE-2024-28074 CVE-2024-23472
- SolarWinds Access Rights Manager (ARM) CreateFile Directory Traversal Remote Code Execution Vulnerability (CVE-2024-23471)
- SolarWinds Access Rights Manager Exposed Dangerous Method Remote Code Execution Vulnerability (CVE-2024-23469)
- SolarWinds Access Rights Manager (ARM) Internal Deserialization Remote Code Execution Vulnerability (CVE-2024-28074)
- SolarWinds ARM Directory Traversal Arbitrary File Deletion and Information Disclosure Vulnerability (CVE-2024-23472)
- SolarWinds Security Vulnerabilities