February 16, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware SolarWinds has patched five remote code execution (RCE) vulnerabilities in the Access Rights Manager (ARM) solution, three of these vulnerabilities are assessed as critical risks. The vulnerability affects versions prior to Access Rights Manager 2023.2.3.

Technical Details

The first two critical vulnerabilities CVE-2024-23476, and CVE-2024-23479, impacting the SolarWinds Access Rights Manager (ARM) were found to be susceptible to a Directory Traversal Remote Code Execution Vulnerability. If exploited, this vulnerability allows an unauthenticated user to achieve the Remote Code Execution. The third critical flaw tracked as CVE-2023-40057 is caused by deserialization of untrusted data. This vulnerability may also allow an unauthenticated to gain remote code execution on targeted systems left unpatched.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists 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.

References

- CVE-2023-40057, CVE-2024-23476, CVE-2024-23477, CVE-2024-23478, CVE-2024-23479
- ARM 2023.2.3 Release Notes
- SolarWinds fixes critical RCE bugs in access rights audit solution
- VRM Vulnerability Reports