Security Advisory 2023-080

Multiple Vulnerabilities in SolarWinds Access Rights Manager (ARM)

October 23, 2023 — v1.0

TLP:CLEAR

History:
- 23/10/2023 — v1.0 – Initial publication

Summary

On October 18 2023, SolarWinds announced patches for eight vulnerabilities in Access Rights Manager (ARM) including eight high-severity flaws. The most severe vulnerabilities are tracked as CVE-2023-35182 and CVE-2023-35184 for Remote Code Execution Vulnerability, as well as CVE-2023-35185 and CVE-2023-35187 for Directory Traversal Remote Code Vulnerability, with a CVSS score of 8.8 out of 10. [1]

It is recommended updating as soon as possible.

Technical Details

Various vulnerabilities were addressed in this patch release, including:

- **CVE-2023-35180**: This vulnerability (CVSS score of 8.0) allows authenticated users to abuse SolarWinds ARM API in order to remotely execute code. [1]
- **CVE-2023-35181**: This vulnerability (CVSS score of 7.8) allows users to abuse incorrect folder permission resulting in privilege escalation. [1]
- **CVE-2023-35182**: This vulnerability (CVSS score of 8.8) can be abused by unauthenticated users on SolarWinds ARM Server resulting in remote code execution. [1]
- **CVE-2023-35183**: This vulnerability (CVSS score of 7.8) allows authenticated users to abuse local resources resulting in privilege escalation. [1]
- **CVE-2023-35184**: This vulnerability (CVSS score of 8.8) allows an unauthenticated user to abuse a SolarWinds service resulting in a remote code execution. [1]
- **CVE-2023-35185**: This vulnerability (CVSS score of 8.8) allows remote attackers to execute arbitrary code on SolarWinds ARM. The specific flaw exists within the `OpenFile` method. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. [1,2]
- **CVE-2023-35186**: This vulnerability (CVSS score of 8.0) allows an authenticated user to abuse SolarWinds service resulting in remote code execution. [1]
- **CVE-2023-35187**: This vulnerability (CVSS score of 8.8) allows remote attackers to execute arbitrary code on SolarWinds ARM. The specific flaw exists within the
OpenClientUpdateFile method. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. [1,3]

Affected Products

Access Rights Manager 2023.2.1 is a service release providing bug and security fixes for release 2023.2, although it doesn’t explicitly list the vulnerable versions. [1]

Recommendations

CERT-EU recommends updating to the latest version as soon as possible.

References