CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

18 July 2024

Multiple SolarWinds Access Rights Manager Vulnerabilities

SolarWinds | Directory Traversal | Access Rights Manager | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple high and critical vulnerabilities affecting SolarWinds Access Rights Manager (ARM).[1] Exploitation of the critical vulnerabilities could provide an attacker remote code execution (RCE) and path traversal capabilities, allowing attackers to execute malicious code remotely or access restricted directories and execute commands outside of the web server's root directory.[1,2]

Affected SolarWinds Product	Issue	CVE Identifier	CVSS v3.1 score
SolarWinds Access Rights Manager (ARM) versions 2023.2.4 and prior	Allows an unauthenticated user to perform arbitrary file deletion and leak sensitive information	CVE-2024-23468	7.6
		CVE-2024-28992	7.6
		CVE-2024-28993	7.6
		CVE-2024-23475	**9.6**
	Allows an authenticated user to arbitrarily read and delete files in ARM	CVE-2024-23472	**9.6**
	Part of a previous vulnerability not completely fixed	CVE-2024-28074	**9.6**
	Allows an unauthenticated user to perform the actions with SYSTEM privileges	CVE-2024-23469	**9.6**
		CVE-2024-23466	**9.6**
	Allows an unauthenticated user to	CVE-2024-23467	**9.6**

CAL-CSIC-202407-006

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP:CLEAR

	perform remote code execution	CVE-2024-23471	**9.6**
	Susceptible to an Arbitrary File Deletion and Information Disclosure vulnerability	CVE-2024-23474	7.6

Table 1: SolarWinds ARM Vulnerabilities (Critical and High)[3]

The Cal-CSIC recommends immediately upgrading all affected SolarWinds ARM products to the current patched versions.

For further information on upgrading affected SolarWinds ARM products, please refer to Security Resources | SolarWinds Trust Center Security Advisories.[3]

Organization, Source, Reference, and Dissemination Information

Organization Description

California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.

Customer Feedback

If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.

Source Summary Statement

This report was compiled from a variety of sources, predominately open-source reporting.

Handling Caveats

Traffic Light Protocol (TLP): Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

Information Needs

HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

[1] Bleeping Computer "SolarWinds fixes 8 critical bugs in access rights audit software;" https://www.bleepingcomputer.com/news/security/solarwinds-fixes-8-critical-bugs-in-access-rights-audit-software/; accessed 18 July 2024

[2] CVE Details; "CVE-2024-28995;" https://www.cvedetails.com/cve/CVE-2024-28995/; accessed 18 July 2024

[3] SolarWinds: "SolarWinds Security Vulnerabilities;" https://www.solarwinds.com/trust-center/security-advisories/; accessed 18 July 2024

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.