Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

TLP:CLEAR
04 March 2024

SolarWinds Security Event Manager Vulnerability

CVE-2024-0692 | SolarWinds | RCE | High Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a high vulnerability known as CVE-2024-0692.[1] The vulnerability affects SolarWinds Security Event Manager versions 2023.0 through 2023.4.[2] The vulnerability is categorized as an unauthenticated Remote Code Execution (RCE) flaw.[3] Exploitation could enable attackers to gain unauthorized access or control over the systems running vulnerable versions of the SolarWinds Security Event Manager.[4]

The Cal-CSIC recommends upgrading to SolarWinds Security Event Manager version 2023.4.1 as soon as possible.

For further information on applying upgrades, please refer to SEM Installation and Upgrade Guide.

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.

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.

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*

[1] National Vulnerability Database; "CVE-2024-0692 Detail;" https://nvd.nist.gov/vuln/detail/CVE-2024-0692; accessed 04 March 2024

[2] SolarWinds; "SolarWinds SEM Deserialization of Untrusted Data Remote Code Execution Vulnerability (CVE-2024-0692);" https://www.solarwinds.com/trust-center/security-advisories/cve-2024-0692; accessed 04 March 2024

[3] Mitre; "CVE-2024-0692;" https://cve.mitre.org/cgi-bin/cvename.cgi?name=2024-0692; accessed 04 March 2024

[4] Vulcan; "How to fix CVE-2024-0692 in SolarWinds Security Event Manager;" https://vulcan.io/blog/how-to-fix-cve-2024-0692-in-solarwinds-security-event-manager/; accessed 04 March 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.