CYBER ADVISORY

TLP:CLEAR

14 August 2024

SolarWinds Web Help Desk

CVE-2024-28986 | SolarWinds | Jave Deserialization | RCE

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a very critical vulnerability known as CVE-2024-28986, with a CVSS v3 score of 9.8.[1,2,3] This vulnerability affects all SolarWinds Web Help Desk (WHD) versions up to 12.8.3.[2,3] Exploitation of this vulnerability allows for Java Deserialization Remote Code Execution, allowing an attacker to remotely run commands on the host machine, and does not require any form of authentication.[1,3]

The Cal-CSIC highly recommends following SolarWind's resolution guide for mitigation.

Further information on SolarWind's mitigation instructions can be found here WHD 12.8.3 Hotfix 1 (solarwinds.com).

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*

[1]VulDB; "SolarWinds Web Help Desk up to 12.8.3 Deserialization" https://vuldb.com/?id.274507; accessed 14 August 2024

[2] Tenable; "CVE-2024-28986" https://www.tenable.com/cve/CVE-2024-28986; accessed 14 August 2024

[3] SolarWinds Customer Service; "WHD 12.8.3 Hotfix 1" https://support.solarwinds.com/SuccessCenter/s/article/WHD-12-8-3-Hotfix-1; accessed 14 August 2024