CYBER ADVISORY

TLP:CLEAR

20 March 2024

Ivanti Standalone Sentry Vulnerability

CVE-2023-41724 | Standalone Sentry | RCE | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2023-41724.[1] The vulnerability affects Ivanti Standalone Sentry supported versions 9.19. 0, 9.18.0, 9.17.0, and older.[2] Exploitation of the vulnerability may allow an unauthenticated threat actor via remote code execution, (RCE) to execute arbitrary commands on the underlying operating system of the appliance within the same physical or logical network. [3]

The Cal-CSIC recommends to immediately patch to the appropriate Ivanti Standalone Sentry supported version.

For further information on applying Ivanti Standalone Sentry patches, please refer to Ivanti Standalone Sentry 9.14.0 - 9.19.1 Release Notes.

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] Bleeping Computer; "Ivanti fixes critical Standalone Sentry bug reported by NATO;" https://www.bleepingcomputer.com/news/security/ivanti-fixes-critical-standalone-sentry-bug-reported-by-nato/; accessed 20 March 2024
[2] Ivanti; "CVE-2023-41724 (Remote Code Execution) for Ivanti Standalone Sentry;" https://forums.ivanti.com/s/article/CVE-2023-41724-Remote-Code-Execution-for-Ivanti-Standalone-Sentry?language=en_US; accessed 20 March 2024
[3] Ivanti; "KB-CVE-2023-41724 (Remote Code Execution) for Ivanti Standalone Sentry;" https://forums.ivanti.com/s/article/KB-CVE-2023-41724-Remote-Code-Execution-for-Ivanti-Standalone-Sentry?language=en_US; accessed 20 March 2024