CYBER ADVISORY

TLP:CLEAR

05 January 2024

Ivanti Endpoint Manager Vulnerability

CVE-2023-39336 | Ivanti | Endpoint Management | Critical Vulnerability

Executive Summary

The California Cyber Threat Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2023-39336.[1,2] The vulnerability affects Ivanti Endpoint Manager EPM 2022 SU4 and all prior versions.[3] If exploited, an attacker with access to the internal network can leverage an unspecified SQL injection to execute arbitrary SQL queries and retrieve output without the need for authentication. This can then allow the attacker control over machines running the EPM agent. While this applies to all instances of MSSQL, when the core server is configured to use Microsoft SQL Express, this might lead to RCE on the core server.

The Cal-CSIC recommends implementing the latest security patch from Ivanti to address this vulnerability.

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 to 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] The Hacker News; 5 January 2024; "Alert: Ivanti Releases Patch for Critical Vulnerability in Endpoint Manager Solution; https://thehackernews.com/2024/01/alert-ivanti-releases-patch-for.html; visited 5 January 2024

[2] BleepingComputer; 4 January 2024; " Ivanti Warns Critical EPM Bug Lets Hackers Hijack Enrolled Devices"; https://www.bleepingcomputer.com/news/security/ivanti-warns-critical-epm-bug-lets-hackers-hijack-enrolled-devices/; visited 5 January 2024

[3] Ivanti; 4 January 2024; "SA-2023-12-19-CVE-2023-39336"; https://forums.ivanti.com/s/article/SA-2023-12-19-CVE-2023-39336?language=en_US; visited 5 January 2024