CYBER ADVISORY

TLP:CLEAR
11 SEP 2024

Ivanti Endpoint Manager 2024 and 2022 SU6 Vulnerabilities

Ivanti | RCE | EPM | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple critical vulnerabilities affecting Ivanti Endpoint Manager (EPM) 2024 and 2022 SU6, with the most severe flaw being CVE-2024-29847.[1,2] Exploitation of these vulnerabilities potentially allow an attacker to achieve remote code execution (RCE) through either deserialization of untrusted data without authentication, or, with admin privileges, utilize SQL injection bugs. [2]

The Cal-CSIC recommends immediately patching affected Ivanti EPMs.

For further information on upgrading affected Ivanti products, please refer to Security Advisory EPM September 2024 for EPM 2024 and EPM 2022 (ivanti.com) [3]

Issue	CVE Identifier(s)	CVSS v3.0
Deserialization of untrusted data in the agent portal of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to achieve remote code execution.	**CVE-2024-29847**	**10 Critical**
An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	**CVE-2024-32840** **CVE-2024-32842** **CVE-2024-32843** **CVE-2024-32845** **CVE-2024-32846** **CVE-2024-32848** **CVE-2024-34779** **CVE-2024-34783** **CVE-2024-34785**	**9.1 Critical**

Table 1: Ivanti CVE's affecting EPM 2024 and 2022 [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 TLP:CLEAR rules, 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] Cyber Security News; "Ivanti Endpoint Manager RCE Vulnerabilities Let Attackers Gain Server Access Remotely" https://cybersecuritynews.com/ivanti-endpoint-manager-rce-vulnerability/; accessed 11 September 2024

[2] Cyber Security News; "Ivanti Patches Critical Vulnerabilities in Endpoint Manager" https://www.securityweek.com/ivanti-patches-critical-vulnerabilities-in-endpoint-manager/; accessed 11 September 2024

[3] Ivanti; "Security Advisory EPM September 2024 for EPM 2024 and EPM 2022;" https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US; accessed 11 September 2024