CYBER ADVISORY

TLP:CLEAR
17 January 2025

Ivanti Endpoint Manager Multiple Vulnerabilities

Ivanti EPM | Path Traversal Flaw | Critical Vulnerabilities | RCE

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple critical and high vulnerabilities in Ivanti's Endpoint Manager (EPM) versions 2024 November security update and prior, in addition to 2022 SU6 November security update and prior [1]. Exploitation of the most critical vulnerability enables an unauthenticated user to access sensitive files and potentially leak information.[2, 3]

Table 1: Ivanti EPM Critical and High Vulnerabilities List

CVE Identifier(s)	Issue	CVSS v3.0
CVE-2024-10811; CVE-2024-13161; CVE-2024-13160; CVE-2024-13159	Absolute path traversal in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a remote unauthenticated user to leak sensitive information.	9.8 (Critical)
CVE-2024-13158	An unbounded resource search path in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a remote user with admin privileges to achieve remote code execution.	7.2 (High)
CVE-2024-13172	Improper signature verification in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a remote unauthenticated user to achieve remote code execution. Local user interaction is required.	7.8 (High)
CVE-2024-13171	Insufficient filename validation in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a remote	7.8 (High)

	unauthenticated user to achieve remote code execution. Local user interaction is required.	
CVE-2024-13170	An out-of-bounds write in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a remote authenticated user to cause a denial of service.	7.5 (High)
CVE-2024-13169	An out-of-bounds read in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a local user to escalate their privileges.	7.8 (High)
CVE-2024-13168; CVE-2024-13167; CVE-2024-13166; CVE-2024-13165	An out-of-bounds write in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a remote unauthenticated user to cause a denial of service.	7.5 (High)
CVE-2024-13164	An uninitialized resource in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a local authenticated user to escalate their privileges.	7.8 (High)
CVE-2024-13163	Deserialization of untrusted data in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a remote unauthenticated user to achieve remote code execution. Local user interaction is required.	7.8 (High)
CVE-2024-13162	SQL injection in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a remote authenticated user with admin privileges to achieve remote code execution. This CVE addresses incomplete fixes from CVE-2024-32848.	7.2 (High)

The Cal-CSIC recommends immediately applying appropriate mitigations or updates to the affected Ivanti product.

For more information on applying the security updates please refer to the Ivanti Security Advisory.

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 here.
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.

[1] Ivanti; "Security Advisory EPM January 2025 for EPM 2024 and EPM 2022 SU6"; https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en_US; accessed 15 January 2025.
[2] National Vulnerability Database; "CVE-2024-10811 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2024-10811; accessed 15 January 2025.
[3] Security Week; "Ivanti Patches Critical Vulnerabilities in Endpoint Manager"; https://www.securityweek.com/ivanti-patches-critical-vulnerabilities-in-endpoint-manager-2/; accessed 15 January 2025.