Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

14 March 2025

Ivanti Endpoint Manager Critical Vulnerabilities Update

Path Traversal Flaw | Proof of Concept | CISA KEV | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of new information regarding three previously published critical vulnerabilities (CVE-2024-13159, CVE-2024-13160, CVE-2024-13161) in Ivanti's Endpoint Manager (EPM) product. All three vulnerabilities are absolute path traversal vulnerabilities in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update, which allow a remote unauthenticated user to leak sensitive information.[1][2][3] Since the publication of our previous Cyber Advisory (serial number CAL-CSIC-202501-008), a proof of concept has been released by a cybersecurity company, Horizon3.ai.[4] Additionally, CISA has added the three vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog.[5]

The Cal-CSIC recommends immediately updating to the latest Ivanti EPM version.

For further information on applying upgrades please refer to 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.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

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] National Vulnerability Database; “CVE-2024-13159 Detail”; https://nvd.nist.gov/vuln/detail/CVE-2024-13159; accessed 13 March 2025.

[2] National Vulnerability Database; “CVE-2024-13160 Detail”; https://nvd.nist.gov/vuln/detail/CVE-2024-13160; accessed 13 March 2025.

[3] National Vulnerability Database; “CVE-2024-13161 Detail”; https://nvd.nist.gov/vuln/detail/CVE-2024-13161; accessed 13 March 2025.

[4] Horizon3.ai; “Ivanti Endpoint Manager – Multiple Credential Coercion Vulnerabilities”; https://www.horizon3.ai/attack-research/attack-blogs/ivanti-endpoint-manager-multiple-credential-coercion-vulnerabilities/; accessed 13 March 2025.

[5] Cybersecurity and Infrastructure Security Agency; “Known Exploited Vulnerabilities Catalog”; https://www.cisa.gov/known-exploited-vulnerabilities-catalog; accessed 13 March 2025.

CAL-CSIC-202503-003

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP:CLEAR