Cal OES
GOVERNOR'S OFFICE OF EMERGENCY SERVICES

CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

25 September 2024

Ivanti Virtual Traffic Manager Vulnerability

CVE-2024-7593 | Ivanti vTM | Active Exploitation | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability under active exploitation known as CVE-2024-7593, with a reported CVSS v3 rating of 9.8.[1] The authentication bypass vulnerability affects Ivanti's Virtual Traffic Manager (vTM).[2] Exploitation of the vulnerability could allow unauthenticated attacker to create an administrator account.[3]

Affected Ivanti vTM Version	Fixed Version
22.2	22.2R1
22.3	22.3R3
22.3R2	22.3R3
22.5R1	22.5R2
22.6R1	22.6R2
22.7R1	22.7R2

Table 1: Affected and Fixed vTM Versions

The Cal-CSIC recommends immediately upgrading to the appropriate fixed Ivanti vTM version.

For further information on applying upgrades please refer to Ivanti Customer Portal.

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

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.

	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] National Vulnerability Database; "CVE-2024-7593 Detail;" https://nvd.nist.gov/vuln/detail/CVE-2024-7593; accessed 25 September 2024

[2] Bleeping Computer; "Critical Ivanti vTM auth bypass bug now exploited in attacks" https://www.bleepingcomputer.com/news/security/critical-ivanti-vtm-auth-bypass-bug-now-exploited-in-attacks/; accessed 25 September 2024

[3] Security Week; "Third Recent Ivanti Vulnerability Exploited in the Wild" https://www.securityweek.com/third-recent-ivanti-product-vulnerability-exploited-in-the-wild/; accessed 25 September 2024

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.