CYBER ADVISORY

TLP:CLEAR
17 April 2024

Ivanti Avalanche MDM Vulnerabilities

CVE-2024-24996 | CVE-2024-29204 | Ivanti | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of critical vulnerabilities known as CVE-2024-24996 and CVE-2024-29204.[1] These vulnerabilities affect Ivanti Avalanche mobile device management (MDM) solution all versions prior to 6.4.3.[2] CVE-2024-24996 lies specifically within Ivanti Avalanche component WLInfoRailService and CVE-2024-29204 lies specifically within Ivanti Avalanche component WLAvalancheService. Both vulnerabilities are caused by heap-based buffer overflow weaknesses, which may allow an unauthenticated remote attacker to execute arbitrary commands on vulnerable systems in low-complexity attacks that do not require user interaction.[3]

The Cal-CSIC recommends immediately upgrading to Ivanti Avalanche MDM version 6.4.3

For further information on applying Ivanti Avalanche MDM upgrades please refer to Ivanti Wavelink.

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 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] Bleeping Computer; "Ivanti warns of critical flaws in its Avalanche MDM solution;" https://www.bleepingcomputer.com/news/security/ivanti-warns-of-critical-flaws-in-its-avalanche-mdm-solution/; accessed 17 April 2024

[2] SOC Radar; "Ivanti Avalanche Received an Update for Over Two Dozen Vulnerabilities (CVE-2024-24996, CVE-2024-29204…);" https://socradar.io/ivanti-avalanche-update-for-two-dozen-vulnerabilities/; accessed 17 April 2024

[3] Ivanti; "Avalanche 6.4.3 Security Hardening and CVEs addressed;" https://forums.ivanti.com/s/article/Avalanche-6-4-3-Security-Hardening-and-CVEs-addressed?language=en_US; accessed 17 April 2024