CYBER ADVISORY

Friday, June 12, 2026 **CAL-CSIC-202606-A-008**

Critical Vulnerabilities Impacting Ivanti Sentry

Remote Code Execution	Full Administrative Access	Proof-of-Concept Available	Patch Available

The Cybersecurity Integration Center (CSIC) has become aware of two critical vulnerabilities impacting Ivanti Sentry. CVE-2026-10520 carries a CVSS 3.1score of 10.0 and CVE-2026-10523 carries a CVSS 3.1 score of 9.9.[1], [2]

CVE-2026-10520 is an OS Command Injection vulnerability that enables a remote, unauthenticated attacker to achieve RCE (Remote Code Execution) with *root* privileges. The vulnerability resides in the *ConfigServiceController* class within the Sentry web application. Successful exploitation exposes the compromised system to backdoor persistence and further malicious code injection into the targeted system.[3]

CVE-2026-10523 is an Authentication Bypass vulnerability that enables a remote, unauthenticated attacker to create arbitrary administrative accounts and obtain full administrative access. Successful exploitation exposes the central point for the network's security monitoring and control. Additionally, it allows the attacker to modify security policy, disable monitoring capability, backdoor creation, and the ability to pivot to other systems within the network.[4]

As of June 9, 2026, Ivanti is not aware of any of their clients being exploited by these vulnerabilities. However, open-source reporting as of June 11, 2026, suggests that threat actors have begun exploiting CVE-2026-10520 right after a Proof-of-Concept[5] was released.[6] Ivanti has issued a security bulletin and have released a patch to address these two vulnerabilities.

The Cal-CSIC recommends following Ivanti's mitigation guidance as soon as possible.[7] Please note that an Ivanti login is required regarding patch availability. For additional details for both CVE-2026-10520 and CVE-2026-10523, please use this link:

Ivanti Security Bulletin and Patch Links: https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2026-10520-CVE-2026-10523?language=en_US

WatchTowr Labs Technical Details: https://labs.watchtowr.com/more-evidence-that-words-dont-mean-what-we-thought-they-meant-ivanti-sentry-pre-auth-os-command-injection-cve-2026-10520/

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Affected Product(s) and Version(s) for both CVEs

Product	Affected Version	Resolved Version
Ivanti Sentry	10.5.1, 10.6.1, 10.7.0 and prior versions	10.5.2, 10.6.2, 10.7.1

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] NVD; "CVE-2026-10520 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-10520; accessed 11 June 2026
[2] NVD; "CVE-2026-10523 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-10523; accessed 11 June 2026
[3] Rapid7; "CVE-2026-10520, CVE-2026-10523 - Multiple critical vulnerabilities affecting Ivanti Sentry"; https://cvefeed.io/vuln/detail/CVE-2026-47938; accessed 11 June 2026
[4] Centre for Cybersecurity Belgium; "Warning: CRITICAL ROOT-LEVEL REMOTE CODE EXECUTION AND AUTHENTICATION BYPASS VULNERABILITIES IN IVANTI SENTRY, Patch Immediately!"; https://cvefeed.io/vuln/detail/CVE-2026-48303; accessed 11 June 2026
[5] Watchtowr Labs; "More Evidence That Words Don't Mean What We Thought They Meant (Ivanti Sentry Pre-Auth OS Command Injection CVE-2026-10520)"; https://labs.watchtowr.com/more-evidence-that-words-dont-mean-what-we-thought-they-meant-ivanti-sentry-pre-auth-os-command-injection-cve-2026-10520/; accessed 11 June 2026
[6] Cyber Security News; "Ivanti Command Injection Vulnerability Exploited in Attacks Following PoC Release"; https://cybersecuritynews.com/ivanti-command-injection-vulnerability-exploit/; accessed 11 June 2026
[7] Ivanti Innovators Hub; "Security Advisory Ivanti Sentry (CVE-2026-10520, CVE-2026-10523)"; https://helpx.adobe.com/security/products/campaign/apsb26-66.html; accessed 11 June 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.