Security Advisory 2026-008

Critical vulnerabilities in Ivanti Sentry

2026-06-10 — v1.0

TLP:CLEAR

History:

- *10/06/2026 — v1.0 – Initial publication*

Summary

On 9 June 2026, Ivanti released a security advisory addressing two critical vulnerabilities in their Sentry products[1]. An attacker could exploit those flaws to achieve unauthenticated remote code execution on the vulnerable device.

Technical Details

The vulnerability **CVE-2026-10520**, with a CVSS score of 10, is an OS Command Injection vulnerability in Ivanti Sentry which allows a remote unauthenticated user to achieve root-level remote code execution[2].

The vulnerability **CVE-2026-10523**, with a CVSS score of 9.9, is an Authentication Bypass vulnerability in Ivanti Sentry which allows a remote unauthenticated attacker to create arbitrary administrative accounts and obtain full administrative access.

Affected Products

The following versions of Ivanti Sentry are affected:

- 10.5.1 and prior.
- 10.6.1 and prior.
- 10.7.0 and prior.

Recommendations

CERT-EU recommends following the vendor's guidance to update their appliance to one of the fixed versions[1].

References

[1] https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2026-10520-CVE-2026-10523

[2] 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/