مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Critical Vulnerabilities in Ivanti Sentry

Tracking #:432319105

Date:10-06-2026



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Ivanti has released security updates to address two critical vulnerabilities affecting Ivanti Sentry.

## TECHNICAL DETAILS:

Ivanti has released security updates to address two critical vulnerabilities affecting Ivanti Sentry. Successful exploitation of these vulnerabilities could allow remote, unauthenticated attackers to achieve root-level remote code execution, bypass authentication mechanisms, create unauthorized administrative accounts, and gain full control of affected Sentry appliances.

**Vulnerability Details:**

1. **CVE-2026-10520 – OS Command Injection Remote Code Execution**
   - **Severity:** Critical (CVSS 10.0)
   - **CWE:** CWE-78 – OS Command Injection

2. **CVE-2026-10523 – Authentication Bypass**
   - **Severity:** Critical (CVSS 9.9)
   - **CWE:** CWE-288 – Authentication Bypass Using an Alternate Path or Channel

**Affected & Fixed Versions:**

| Product | Affected Versions | Fixed Versions |
|---|---|---|
| Ivanti Sentry | 10.5.1 and earlier, 10.6.1 and earlier, 10.7.0 and earlier | 10.5.2, 10.6.2, 10.7.1 |

## RECOMMENDATIONS:

**Immediate Actions**

- Upgrade affected Ivanti Sentry appliances to fixed version.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

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