10 years CERT-EU

### Security Advisory 2024-002

# Critical Vulnerability in Ivanti Endpoint Management Software

*January 8, 2024 — v1.0*

**TLP:CLEAR**

*History:*

- *08/01/2024 — v1.0 – Initial publication*

## Summary

On January 4th, 2024, a critical remote code execution (RCE) vulnerability was fixed in Ivanti's Endpoint Management software (EPM). This vulnerability, tracked as `CVE-2023-39336` (CVSS score : 9.6), allows unauthenticated attackers to hijack enrolled devices or the core server. Ivanti EPM is used to manage client devices across various platforms, including Windows, macOS, Chrome OS, and IoT operating systems. The vulnerability affects all supported versions of Ivanti EPM and has been resolved in version 2022 Service Update 5. The editor also states that no evidence of active exploitation was currently found.

## Technical Details

The vulnerability allows attackers with access to a target's internal network to exploit the flaw in low-complexity attacks without requiring privileges or user interaction. It involves an unspecified SQL injection, enabling attackers to execute arbitrary SQL queries and retrieve output without authentication. This vulnerability could lead to attackers gaining control over machines running the EPM agent, and potentially remote code execution on the core server if configured with SQL express.

## Affected Products

All supported versions of Ivanti Endpoint Management software (EPM) prior to version 2022 Service Update 5.

## Recommendations

CERT-EU recommends updating to version 2022 Service Update 5 to mitigate this vulnerability as soon as possible.

## References

[1] https://www.bleepingcomputer.com/news/security/ivanti-warns-critical-epm-bug-lets-hackers-hijack-enrolled-devices/