Security Advisory 2026-001

Critical vulnerabilities in Ivanti EPMM

2026-01-30 — v1.0

TLP:CLEAR

History:

- *30/01/2026 — v1.0 – Initial publication*

Summary

On 29 January 2026, Ivanti released a security advisory addressing two critical vulnerabilities in their EPMM products. An attacker could exploit those flaws to achieve unauthenticated remote code execution on the vulnerable device. One of these vulnerabilities have been exploited in a limited number of cases [1].

Technical Details

The vulnerability **CVE-2026-1281**, with a CVSS score of 9.8, is a code injection vulnerability in Ivanti Endpoint Manager Mobile.

The vulnerability **CVE-2026-1340**, with a CVSS score of 9.8, is a code injection vulnerability in Ivanti Endpoint Manager Mobile.

Affected Products

The following versions of Ivanti's Endpoint Manager Mobile (EPMM) are affected:

- 12.5.1.0 and prior.
- 12.6.1.0 and prior.
- 12.7.0.0 and prior.

Recommendations

CERT-EU recommends securing forensic evidence to detect any signs of exploitation. CERT-EU also recommends following the vendor's guidance to apply the hotfix (i.e. RPM 12.x.0 or RPM 12.x.1) on vulnerable appliances. As noted by the vendor, the applied RPM script will not survive a version upgrade which means that the script will need to be reapplied after an upgrade to a new version. The permanent fix for this vulnerability will be included in the release 12.8.0.0 which is planned for Q1 2026.

References

[1] https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US