



An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2601300200

NCSC Advisory

Ivanti: Endpoint Manager Mobile Critical CVE-2026-1281, CVE-2026-1340

30th, January 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see <https://www.first.org/tmlp/>. Please treat this document in accordance with the TLP assigned.



Description

CVE ID: CVE-2026-1281**Published:** 2026-01-29**Vendor:** Ivanti**Product:** Endpoint Manager Mobile**CVSS Score¹:** 9.8**Known Exploited Vulnerability (KEV) catalog²:** Yes**CVE ID:** CVE-2026-1340**Published:** 2026-01-29**Vendor:** Ivanti**Product:** Endpoint Manager Mobile**CVSS Score:** 9.8**Known Exploited Vulnerability (KEV) catalog:** No

Products Affected

| Product | Version | Patches |
|--------------------------------|--|---|
| Ivanti Endpoint Manager Mobile | 12.5.0.0 and prior 12.6.0.0 and prior 12.7.0.0 and prior | https://support.mobileiron.com/mi/vsp/AB1771634/ivanti-security-update-1761642-1.0.0S-5.noarch.rpm |
| Ivanti Endpoint Manager Mobile | 12.5.1.0 and prior 12.6.1.0 and prior | https://support.mobileiron.com/mi/vsp/AB1771634/ivanti-security-update-1761642-1.0.0L-5.noarch.rpm |

Impact

A critical code injection vulnerability in Ivanti Endpoint Manager Mobile allowing attackers to achieve unauthenticated remote code execution., CAPEC-242 Code Injection.

¹ <https://www.first.org/cvss/>

² <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



Common Weakness Enumeration (CWE)³: CWE-94: Improper Control of Generation of Code ('Code Injection')

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Ivanti.

- <https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340>
- https://forums.ivanti.com/s/article/Analysis-Guidance-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US&_gl=1*11h511z*_gcl_au*MTA3OTkxMjYzMC4xNzY5Njk5MTgw
- <https://nvd.nist.gov/vuln/detail/CVE-2026-1281>
- <https://nvd.nist.gov/vuln/detail/CVE-2026-1340>
- <https://www.cve.org/CVERecord?id=CVE-2026-1281>
- <https://www.cve.org/CVERecord?id=CVE-2026-1340>
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-1281

³ <https://cwe.mitre.org>