An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2505140002

NCSC Advisory

Critical Vulnerability found in Ivanti Endpoint Manager Mobile (EPMM)

14th, May 2025

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/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID and CVSS Score:

- CVE-2025-4428 (CVSS: 7.2)
- CVE-2025-4427 (CVSS: 5.3)

Published: 2025-05-13

Vendor: Ivanti

Product: Endpoint Manager Mobile

Products Affected

Product	Version
Ivanti Endpoint Manager Mobile	11.12.0.4 and prior 12.3.0.1 and prior 12.4.0.1 and prior 12.5.0.0 and prior

Impact

Ivanti has released updates for Endpoint Manager Mobile (EPMM) which addresses one medium and one high severity vulnerability. When chained together, successful exploitation could lead to unauthenticated remote code execution. Remote Code Execution in the API component of Ivanti Endpoint Manager Mobile 12.5.0.0 and prior, allows authenticated attackers to execute arbitrary code via crafted API requests. Ivanti are aware of a very limited number of customers whose solution has been exploited at the time of disclosure.

Common Weakness Enumeration (CWE)[1]:

CWE-94: Improper Control of Generation of Code ('Code Injection')

CWE-288: Authentication Bypass Using an Alternate Path or Channel

Known Exploited Vulnerability (KEV) catalog[2]: No

Used by Ransomware Operators: N/A

[1] https://cwe.mitre.org

[2] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

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://nvd.nist.gov/vuln/detail/CVE-2025-4428
- https://www.cve.org/CVERecord?id=CVE-2025-4428
- https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM