An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2605080214

NCSC Advisory

Multiple Vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM)

8th, May 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/tlp/. Please treat this document in accordance with the TLP assigned.

An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

Description

CVE ID: CVE-2026-5786, CVE-2026-5787, CVE-2026-5788, CVE-2026-6973, CVE-2026-7821

Published: 2026-05-07

Vendor: Ivanti

CVE-2026-5786

Products Affected

Product	Version
Ivanti Endpoint Manager Mobile (EPMM)	<12.8.0.1
Ivanti Endpoint Manager Mobile (EPMM)	<12.7.0.1
Ivanti Endpoint Manager Mobile (EPMM)	<12.6.1.1

Impact

An Improper Access Control vulnerability in Ivanti EPMM before versions 12.6.1.1, 12.7.0.1, and 12.8.0.1 allows a remote authenticated attacker to gain administrative access. CAPEC-233 Privilege Escalation

CVSS Score[1]: 8.8

Common Weakness Enumeration (CWE)[2]: CWE-284: Improper Access Control

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/

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

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

An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

CVE-2026-5787

Products Affected

Product	Version
Ivanti Endpoint Manager Mobile (EPMM)	<12.8.0.1
Ivanti Endpoint Manager Mobile (EPMM)	<12.7.0.1
Ivanti Endpoint Manager Mobile (EPMM)	<12.6.1.1

Impact

An Improper Certificate Validation in Ivanti EPMM before versions 12.6.1.1, 12.7.0.1, and 12.8.0.1 allows a remote unauthenticated attacker to impersonate registered Sentry hosts and obtain valid CA-signed client certificates. CAPEC-196 Session Credential Falsification through Forging

CVSS Score: 8.9

Common Weakness Enumeration (CWE): CWE-295: Improper certificate validation

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

CVE-2026-5788

Products Affected

Product	Version
Ivanti Endpoint Manager Mobile (EPMM)	<12.8.0.1
Ivanti Endpoint Manager Mobile (EPMM)	<12.7.0.1
Ivanti Endpoint Manager Mobile (EPMM)	<12.6.1.1

Impact

An Improper Access Control in Ivanti EPMM before versions 12.6.1.1, 12.7.0.1, and 12.8.0.1 allows a remote unauthenticated attacker to invoke arbitrary methods. CAPEC-115 Authentication Bypass

CVSS Score: 7.0

Common Weakness Enumeration (CWE): CWE-284: Improper Access Control

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

CVE-2026-6973

Products Affected

Product	Version
Ivanti Endpoint Manager Mobile (EPMM)	<12.8.0.1
Ivanti Endpoint Manager Mobile (EPMM)	<12.7.0.1
Ivanti Endpoint Manager Mobile (EPMM)	<12.6.1.1

Impact

An Improper Input Validation in Ivanti EPMM before versions 12.6.1.1, 12.7.0.1, and 12.8.0.1 allows a remotely authenticated user with administrative access to achieve remote code execution. CAPEC-88 OS Command Injection

CVSS Score: 7.2

Common Weakness Enumeration (CWE): CWE-20: Improper input validation

Known Exploited Vulnerability (KEV) catalog: Yes

Used by Ransomware Operators: N/A

CVE-2026-7821

Products Affected

Product	Version
Ivanti Endpoint Manager Mobile (EPMM)	<12.8.0.1
Ivanti Endpoint Manager Mobile (EPMM)	<12.7.0.1
Ivanti Endpoint Manager Mobile (EPMM)	<12.6.1.1

Impact

Improper certificate validation in Ivanti EPMM before versions 12.6.1.1, 12.7.0.1, and 12.8.0.1 allows a remote unauthenticated attacker to enroll a device belonging to a restricted set of unenrolled devices, leading to information disclosure about EPMM appliance and impacting on the integrity of the newly enrolled device identity. CAPEC-22: Exploiting Trust in Client

CVSS Score: 7.4

Common Weakness Enumeration (CWE): CWE-295: Improper certificate validation

Known Exploited Vulnerability (KEV) catalog: No

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://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs
- https://nvd.nist.gov/vuln/detail/CVE-2026-5786
- https://www.cve.org/CVERecord?id=CVE-2026-5786
- https://nvd.nist.gov/vuln/detail/CVE-2026-5787
- https://www.cve.org/CVERecord?id=CVE-2026-5787
- https://nvd.nist.gov/vuln/detail/CVE-2026-5788
- https://www.cve.org/CVERecord?id=CVE-2026-5788
- https://nvd.nist.gov/vuln/detail/CVE-2026-6973
- https://www.cve.org/CVERecord?id=CVE-2026-6973
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-6973
- https://nvd.nist.gov/vuln/detail/CVE-2026-7821
- https://www.cve.org/CVERecord?id=CVE-2026-7821