



Ivanti Endpoint Manager Mobile (EPMM) Path Traversal Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-35081
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-03 18:15:00 UTC
Updated	2023-08-08 20:25:00 UTC
Description	A path traversal vulnerability in Ivanti EPMM versions (11.10.x < 11.10.0.3, 11.9.x < 11.9.1.2 and 11.8.x < 11.8.1.2) allows a

Risk And Classification

EPSS: 0.913710000 probability, percentile 0.996640000 (date 2026-04-22)

CISA KEV: Listed on 2023-07-31; due 2023-08-21; ransomware use Unknown

Problem Types: CWE-22

CISA Known Exploited Vulnerability

Vendor	Ivanti
Product	Endpoint Manager Mobile (EPMM)
Name	Ivanti Endpoint Manager Mobile (EPMM) Path Traversal Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	https://forums.ivanti.com/s/article/CVE-2023-35081-Arbitrary-File-Write?language=en_US ; https://nvd.nist.gov/vuln/detail/CVE-2023-35081

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ivanti	Endpoint Manager Mobile	All	All	All	All

References

Reference	Source	Link	Tags
Ivanti Community	MISC	forums.ivanti.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[730859](#) Ivanti Endpoint Manager Mobile (EPMM) Remote Arbitrary File Write Vulnerability

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report