National Cyber Security Centre

2307250110-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Vulnerability advisory for Ivanti EPMM - formerly known as MobileIron Core

Tuesday 25th July, 2023

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.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

Ivanti have disclosed details of a remote unauthenticated API access vulnerability in Ivanti Endpoint Manager Mobile (EPMM), formerly known as MobileIron Core, that impacts all supported versions of the product as well as end-of-life versions. This vulnerability is being tracked as CVE-2023-35078 and has been assigned a CVSS of 10.0. Advice for administrators is available from Ivanti here: https://forums.ivanti.com/s/article/CVE-2023-35078-Remote-unauthenticated-API-access-vulnerability?language=en_US

Products Affected

All supported versions are affected:

- Ivanti Endpoint Manager Mobile versions 11.4, 11.10, 11.9 11.8
- Older versions/releases are also vulnerable

Impact

Successful exploitation of this vulnerability could allow an unauthenticated remote actor to access users' Personally Identifiable Information (PII) and to add an administrative account and/or change the configuration. Ivanti are aware of a number of customers that have been impacted.

Recommendations

Ivanti have released a patch to remediate this vulnerability and recommend that customers apply this immediately. Information on how to access the patch and apply remediation's are available to Ivanti customers by logging in to the customer portal here: https://forums.ivanti.com/s/article/KB-Remote-unauthenticated-API-access-vulnerability-CVE-2023-35078

The NCSC strongly advises affected organisations to follow Ivanti's advice and take immediate steps to remediate this vulnerability by upgrading. If you cannot upgrade, please refer to the information in the advisory to apply an RPM-based solution.

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie