



NCSC-2025-0152

Kwetsbaarheden verholpen in Ivanti Endpoint Manager Mobile (EPMM, voormalig MobileIron)

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 13-05-2025

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Ivanti heeft kwetsbaarheden verholpen in de Ivanti Endpoint Manager Mobile (EPMM, voorheen MobileIron). Alleen de On-prem versies van de EPMM zijn kwetsbaar.

Duiding

De kwetsbaarheden betreffen een authentication bypass en remote code execution die gezamenlijk misbruikt kunnen worden om op afstand code uit te voeren op Ivanti Endpoint Manager Mobile (EPMM). Middels deze kwetsbaarheden kan een kwaadwillende inloggen in de Ivanti Endpoint Manager Mobile (EPMM) en mogelijk toegang krijgen tot gevoelige gegevens. Het NCSC heeft uit betrouwbare bron vernomen dat reeds selectief misbruik van deze kwetsbaarheden heeft plaatsgevonden. Het risico bestaat dat kort na de publicatie van Ivanti een publieke PoC online komt wat het risico op misbruik zou vergroten.

Oplossingen

Ivanti heeft updates uitgebracht om de kwetsbaarheden in Ivanti Endpoint Manager Mobile (EPMM, voorheen MobileIron) versies te verhelpen. Ivanti geeft het advies voor gebruikers van de On-prem versie van de Endpoint Manager Mobile om te updaten naar de nieuwste versie. Zie de referentie voor meer informatie.

De getroffen versies waarvoor updates beschikbaar zijn: < 11.12.0.4 updaten naar 11.12.0.5, < 12.3.0.1 updaten naar 12.3.0.2, < 12.4.0.1 updaten naar 12.4.0.2, < 12.5.0.0 updaten naar 12.5.0.1

Referenties

- <https://www.cve.org/CVERecord?id=CVE-2025-4427>
- <https://www.cve.org/CVERecord?id=CVE-2025-4428>
- <https://www.ivanti.com/blog/epmm-security-update>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-4428	
➤ CVE-2025-4427	

CWE's

CWE	Beschrijving
> CWE-288	Authentication Bypass Using an Alternate Path or Channel
> CWE-94	Improper Control of Generation of Code ('Code Injection')

Getroffen producten

Ivanti
Endpoint Manager Mobile

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.