



NCSC-2026-0043

Zeroday-kwetsbaarheden verholpen in Ivanti Endpoint Manager Mobile

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 20-02-2026

Revisie: 1.0.2

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

Update Revisie 2

Voor de kwetsbaarheid met kenmerk CVE-2026-1281 is Proof-of-Concept-code (PoC) gepubliceerd. Dit vergroot de kans op misbruik van de kwetsbaarheid aanzienlijk.

Feiten

Ivanti heeft twee kwetsbaarheden verholpen in Endpoint Manager Mobile (EPMM), ook wel bekend als MobileIron.

Duiding

De kwetsbaarheden stellen een ongeauthenticeerde kwaadwillende in staat om willekeurige code uit te voeren op het kwetsbare systeem.

Van de kwetsbaarheid met kenmerk CVE-2026-1281 meldt Ivanti dat deze actief is misbruikt bij een zeer beperkt aantal klanten.

Er is Proof-of-Concept-code publiek beschikbaar. Dit vergroot de kans grootschalig misbruik aanzienlijk.

Update: Afhankelijk van de configuratie van EPMM kan deze toegang verlenen tot het Sentry systeem. Hierdoor kan compromittatie van het EPMM systeem kwaadwillenden mogelijk toegang tot het Sentry systeem verschaffen. Hiervoor is toegang tot de keystore op het EPMM systeem vereist. Onderzoek het Sentry systeem op verdachte toegang en verdacht verkeer vanaf EPMM.

Oplossingen

Ivanti heeft updates beschikbaar gesteld om de kwetsbaarheden te verhelpen. Lees het beveiligingsadvies van Ivanti en het websitebericht van het NCSC voor meer informatie. Referenties hiernaar vind je in onderstaande referentielijst.

Referenties

➤ <https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340>

➤ <https://www.ncsc.nl/waarschuwing/ncsc-roept-organisaties-op-zich-te-melden-bij-gebruik-van-ivanti-endpoint-manager>

Kwetsbaarheden

CVE	CVSS Score
> CVE-2026-1281	6.9 MEDIUM
> CVE-2026-1340	9.3 CRITICAL

CWE's

CWE	Beschrijving
> 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.