Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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