Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0135

Kwetsbaarheden verholpen in Ivanti Endpoint Manager Mobile

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 07-05-2026

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

Duiding

De kwetsbaarheid met het kenmerk CVE-2026-6973 stelt een geauthenticeerde kwaadwillende met administratieve toegang in staat om op afstand willekeurige code uit te voeren met beheerdersrechten. Van de kwetsbaarheid met kenmerk CVE-2026-6973 meldt Ivanti dat deze actief is misbruikt bij een zeer beperkt aantal klanten. Om succesvol misbruik te bewerkstelligen moet de kwaadwillende beschikken over valide inloggegevens van een account met adminrechten. Ivanti geeft aan dat klanten die het advies in januari hebben opgevolgd om hun inloggegevens te vernieuwen, aanzienlijk minder risico lopen.

De kwetsbaarheid met CVE-2026-5786 stelt een geauthenticeerde kwaadwillende op afstand in staat om beheertoegang te verkrijgen. De kwetsbaarheid met CVE-2026-5787 stelt een niet-geauthenticeerde kwaadwillende in staat om zich voor te doen als een geregistreerd Sentry systeem, om zodoende door een Certificate Authority (CA) ondertekende client certificaten te verkrijgen. De kwetsbaarheid CVE-2026-5788 stelt een niet-geauthenticeerde kwaadwillende op afstand in staat om willekeurige code uit te voeren. De kwetsbaarheid CVE-2026-7821 stelt een niet-geauthenticeerde kwaadwillende in staat om een apparaat te registreren aan een set van niet-geregistreerde apparaten en toegang te verkrijgen tot (gevoelige) gegevens.

Het NCSC verwacht dat op korte termijn Proof-of-Concept code publiek beschikbaar komt. Dit vergroot de kans grootschalig misbruik aanzienlijk.

Oplossingen

Ivanti heeft updates beschikbaar gesteld om de kwetsbaarheden te verhelpen. Lees het beveiligingsadvies van Ivanti in onderstaande referentie voor meer informatie.

Referenties

› https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs?language=en_US

Kwetsbaarheden

CVE	CVSS Score
› CVE-2026-5786	8.8 HIGH

- CVE-2026-5787
- CVE-2026-5788
- CVE-2026-6973
- CVE-2026-7821

CWE's

CWE	Beschrijving
CWE-284	Improper Access Control
CWE-20	Improper Input Validation
CWE-306	Missing Authentication for Critical Function
CWE-295	Improper Certificate Validation

Getroffen producten

Ivanti
Endpoint Manager Mobile

Disclaimer