Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0493 revisie 1.0.1

PRIORITEIT: NORMAAL

# Kwetsbaarheden verholpen in Ivanti Endpoint Manager

Publicatiedatum: 13-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

# Update Revisie

Publieke PoC code verschenen voor CVE-2026-121653.

# Feiten

Ivanti heeft twee kwetsbaarheden in Ivanti Endpoint Manager verholpen, die betrekking hebben op de Core- en Agent-componenten.

# Duiding

De eerste kwetsbaarheid (CVE-2026-121653) betreft een SQL-injectie in de Core van Ivanti Endpoint Manager-versies vóór 2024 SU8. Hierdoor kan een externe, niet-geauthenticeerde aanvaller kwaadaardige SQL-commando's injecteren, wat kan leiden tot het uitvoeren van willekeurige code op afstand (Remote Code Execution, RCE).

De tweede kwetsbaarheid (CVE-2026-18128) betreft het verzenden van gevoelige informatie in cleartext door de Agent van Ivanti Endpoint Manager-versies vóór 2024 SU8. Hierdoor kan een externe, niet-geauthenticeerde aanvaller die zich in een man-in-the-middlepositie (MITM) bevindt, HTTP-verkeer onderscheppen, uitlezen en manipuleren. Dit kan de vertrouwelijkheid en integriteit van de communicatie aantasten.

Update:

Inmiddels is publieke PoC code voor CVE-2026-121653 te vinden op het internet. Dit verhoogt de kans dat deze kwetsbaarheid op korte termijn actief misbruikt zal worden.

# Oplossingen

Ivanti heeft updates uitgebracht om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

# Referenties

- https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-EPM-November-2026?language=en_US

# Kwetsbaarheden

| CVE | CVSS Score |
|---|---|
| CVE-2026-121653 | 9.8 CRITICAL |
| CVE-2026-18128 | 6.8 MEDIUM |

# CWE's

| CWE | Beschrijving |
|---|---|
| CWE-89 | Improper Neutralization of Special Elements used in an SQL Command |
| CWE-319 | Cleartext Transmission of Sensitive Information |

# Getroffen producten

| Ivanti |
|---|
| Endpoint Manager |

# 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.