



# NCSC-2025-0318

## Kwetsbaarheden verholpen in Ivanti Endpoint Manager

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 15-10-2025

**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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Ivanti heeft kwetsbaarheden verholpen in Ivanti Endpoint Manager.

## Duiding

De kwetsbaarheden omvatten een onveilige deserialisatie, een pad-traversal en meerdere SQL-injectie kwetsbaarheden. De onveilige deserialisatie kan door lokale, geauthenticeerde aanvallers worden misbruikt om verhoogde privileges te verkrijgen, wat leidt tot ongeautoriseerde toegang tot gevoelige functionaliteiten en gegevens binnen het systeem. De pad-traversal kwetsbaarheid stelt externe, ongeauthenticeerde aanvallers in staat om willekeurige code uit te voeren op getroffen systemen, wat kan resulteren in ongeautoriseerde toegang en controle over het systeem. De SQL-injectie kwetsbaarheden stellen geauthenticeerde aanvallers in staat om willekeurige SQL-query's tegen de database uit te voeren, wat kan leiden tot ongeautoriseerde toegang tot gevoelige gegevens en compromittering van de integriteit en vertrouwelijkheid van opgeslagen informatie.

## Oplossingen

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

## Referenties

➤ <https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-EPM-October-2025>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2025-11622</a>	8.5 HIGH
➤ <a href="#">CVE-2025-9713</a>	5.3 MEDIUM
➤ <a href="#">CVE-2025-11623</a>	5.3 MEDIUM
➤ <a href="#">CVE-2025-62392</a>	5.3 MEDIUM
➤ <a href="#">CVE-2025-62390</a>	5.3 MEDIUM
➤ <a href="#">CVE-2025-62389</a>	5.3 MEDIUM

> CVE-2025-62388	5.3 MEDIUM
> CVE-2025-62387	5.3 MEDIUM
> CVE-2025-62385	5.3 MEDIUM
> CVE-2025-62391	5.3 MEDIUM
> CVE-2025-62383	5.3 MEDIUM
> CVE-2025-62386	5.3 MEDIUM
> CVE-2025-62384	5.3 MEDIUM

## CWE's

CWE	Beschrijving
> CVE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CVE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
> CVE-502	Deserialization of Untrusted Data

## Getroffen producten

<b>Ivanti</b>
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.