



# NCSC-2025-0253

## Kwetsbaarheden verholpen in Ivanti Connect Secure, Policy Secure en ZTA Gateways

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-08-2025

### **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 Connect Secure, Policy Secure en ZTA Gateways.

## Duiding

De kwetsbaarheden omvatten een buffer over-read en een heap-gebaseerde buffer overflow, die beide kunnen worden misbruikt door remote ongeauthenticeerde aanvallers om een Denial-of-Service (DoS) te veroorzaken. Daarnaast is er een probleem met de onjuiste behandeling van symbolische links, waardoor lokale geauthenticeerde aanvallers toegang kunnen krijgen tot willekeurige bestanden op de schijf, wat kan leiden tot ongeautoriseerde toegang tot gevoelige informatie.

## Oplossingen

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

## Referenties

➤ [https://forums.ivanti.com/s/article/August-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-Multiple-CVEs?language=en\\_US](https://forums.ivanti.com/s/article/August-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-Multiple-CVEs?language=en_US)

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2025-5456</a>	7.5 HIGH
➤ <a href="#">CVE-2025-5462</a>	8.7 HIGH
➤ <a href="#">CVE-2025-5466</a>	5.1 MEDIUM
➤ <a href="#">CVE-2025-5468</a>	5.5 MEDIUM

## CWE's

CWE	Beschrijving
➤ <a href="#">CWE-776</a>	

Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')

- |                           |  |
|---------------------------|--|
| ➤ <a href="#">CWE-61</a>  | UNIX Symbolic Link (Symlink) Following |
| ➤ <a href="#">CWE-125</a> | Out-of-bounds Read                     |
| ➤ <a href="#">CWE-122</a> | Heap-based Buffer Overflow             |

## Getroffen producten

### Ivanti

Connect  
Secure

Neurons for  
Secure

Neurons for Secure  
Access

Policy  
Secure

ZTA  
Gateway

## 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.