



NCSC-2025-0292

Kwetsbaarheden verholpen in Ivanti producten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 16-09-2025

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Ivanti heeft kwetsbaarheden verholpen in meerdere producten zoals Connect Secure en Policy Secure.

Duiding

De kwetsbaarheden bevinden zich in verschillende Ivanti producten en stellen remote geauthenticeerde aanvallers met read-only admin rechten in staat om authenticatie-instellingen te wijzigen, beperkte instellingen te configureren, bestaande HTML5-verbindingen te kapen, en CSRF-aanvallen uit te voeren. Dit kan leiden tot ongeautoriseerde wijzigingen in systeemconfiguraties, ongeautoriseerde toegang en manipulatie van actieve sessies, en het uitvoeren van gevoelige acties namens gebruikers. Daarnaast kunnen aanvallers met admin-rechten een denial-of-service conditie triggeren en interne services enumereren. Een kritieke kwetsbaarheid in Ivanti Connect Secure en andere producten stelt aanvallers in staat om willekeurige tekst in HTTP-responses te injecteren, wat gebruikersinteractie vereist voor exploitatie.

Oplossingen

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

Referenties

➤ <https://forums.ivanti.com/s/article/September-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-and-Neurons-for-Secure-Access-Multiple-CVEs>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-55141	8.8 HIGH
➤ CVE-2025-55142	8.8 HIGH
➤ CVE-2025-55144	5.4 MEDIUM
➤ CVE-2025-55148	7.6 HIGH
➤ CVE-2025-8712	5.4 MEDIUM
➤ CVE-2025-55145	8.9 HIGH

> CVE-2025-55147	8.8 HIGH
> CVE-2025-8711	5.4 MEDIUM
> CVE-2025-55146	4.9 MEDIUM
> CVE-2025-55139	6.8 MEDIUM
> CVE-2025-55143	6.1 MEDIUM

CWE's

CWE	Beschrijving
> CVE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CVE-252	Unchecked Return Value
> CVE-352	Cross-Site Request Forgery (CSRF)
> CVE-862	Missing Authorization
> CVE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

Ivanti
Connect Secure
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.