Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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

Getroffen producten

Ivanti
Connect Secure
Policy Secure
ZTA Gateway

Disclaimer