Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op 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

Kwetsbaarheden

CVE	CVSS Score
› CVE-2025-5456	7.5 HIGH
› CVE-2025-5462	8.7 HIGH
› CVE-2025-5466	5.1 MEDIUM
› CVE-2025-5468	5.5 MEDIUM

CWE's

CWE	Beschrijving
› CWE-776	

Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	
CWE-61	UNIX Symbolic Link (Symlink) Following
CWE-125	Out-of-bounds Read
CWE-122	Heap-based Buffer Overflow

Getroffen producten

Ivanti
Connect Secure
Neurons for Secure
Neurons for Secure Access
Policy Secure
ZTA Gateway

Disclaimer