Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0105

Kwetsbaarheid verholpen in Ivanti Connect Secure, Policy Secure en ZTA Gateways

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 03-04-2025

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 een kwetsbaarheid verholpen in Connect Secure, Policy Secure en ZTA Gateways.

Duiding

Een kwaadwillende kan de kwetsbaarheid misbruiken om willekeurige code uit te voeren op het kwetsbare systeem zonder voorafgaande authenticatie.

Ivanti meldt informatie te hebben dat de kwetsbaarheid beperkt is misbruikt op Connect Secure en Pulse Connect Secure systemen. Pulse Connect Secure is sinds 31 december 2024 End-of-Life en End-of-Support. Er zijn echter nog veel van deze End-of-Life systemen actief in gebruik en vindbaar op Internet. Dit is voor het NCSC de reden om dit beveiligingsadvies in te schalen als **HIGH/HIGH**.

Ivanti meldt dat er voor zover bekend geen misbruik heeft plaatsgevonden op Policy Secure en ZTA Gateway systemen, omdat deze systemen niet zichtbaar zijn vanaf internet, of aanvullende maatregelen hebben die de kans op misbruik zeer klein maakt.

Oplossingen

Pulse Connect Secure appliances 9.1x krijgen **geen** updates, omdat deze productlijn **End-of-Life** en **End-of-Support** is. Het NCSC adviseert om deze systemen niet meer te gebruiken, uit te schakelen en te vervangen door ondersteunde systemen. Neem hiervoor contact op met de leverancier.

Ivanti heeft updates beschikbaar gesteld voor Connect Secure, door versie 22.7R2.6 uit te brengen. Deze update is 11 februari 2025 vrijgegeven. De kwetsbaarheid is daarin verholpen als reguliere bug. Het NCSC heeft hiervoor op 12 februari beveiligingsadvies NCSC-2025-0052 gepubliceerd. Organisaties die dit beveiligingsadvies hebben opgevolgd zijn daardoor niet (meer) kwetsbaar.

Voor Policy Secure is een update in ontwikkeling. Deze wordt 21 april verwacht.

Voor ZTA Gateway is een update in ontwikkeling. Deze wordt 19 april verwacht.

Het risico van actief misbruik is voor de laatstgenoemde systemen sterk gereduceerd vanwege additionele maatregelen die reeds in deze producten zijn geïmplementeerd. Raadpleeg de informatie van Ivanti voor eventuele additionele handelingsperspectieven.

Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://advisories.ncsc.nl/advisory?id=NCSC-2025-0052
- https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457?language=en_US

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-22457	

CWE's

CWE	Beschrijving
CWE-121	Stack-based Buffer Overflow
CWE-319	Cleartext Transmission of Sensitive Information

Disclaimer