Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0398

Kwetsbaarheden verholpen in Ivanti Connect Secure en Policy Secure

2024-10-11 Revisie 1

Updates

Revision: 0

Initiele versie

Revision: 1

POC code beschikbaar voor deze kwetsbaarheid.

Toegestande verspreiding: 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.firs t.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Ivanti heeft een kwetsbaarheid verholpen in Connect Secure en Policy Secure.

Interpretaties

UPDATE: Er is inmiddels POC code online beschikbaar voor deze kwetsbaarheid.

Een geauthenticeerde kwaadwillende met toegang tot de admin portal van Connect Secure of Policy Secure kan de kwetsbaarheid misbruiken om op afstand code uit te voeren.

Ivanti meldt dat er geen indicatie is dat deze kwetsbaarheid wordt misbruikt.

Oplossingen

Ivanti heeft fixes uitgebracht om de kwetsbaarheid te verhelpen voor Connect Secure versies 22.7R2.1 en 22.7R2.2 en Ivanti Policy Secure 22.7R1.1. Voor Connect Secure versie 9.1R18.9 is nog geen fix beschikbaar, deze zal naar verwachting op 15 oktober worden gepubliceerd.

Referenties

- https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-and-Policy-Secure-CVE-2024-37404