



Advisory NCSC-2024-0369

Kwetsbaarheden verholpen in Ivanti Endpoint Manager

2024-09-13 Revisie 1

Updates

Revision: 0

Initiele versie

Revision: 1

New revision

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 kwetsbaarheden verholpen in Ivanti Endpoint Manager.

Interpretaties

Er zijn kwetsbaarheden verholpen in Ivanti Endpoint Manager. Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- (Remote) code execution (Administrator/Root rechten)
- Toegang tot systeemgegevens
- Verhoogde gebruikersrechten

Ivanti heeft geen aanwijzingen dat er actief misbruik plaatsvindt van deze kwetsbaarheden.

Onderzoekers hebben Proof-of-Concept-code gepubliceerd, waarmee de kwetsbaarheid met kenmerk CVE-2024-29847 kan worden aangetoond. Het is goed gebruik een dergelijke interface niet publiek toegankelijk te hebben, maar af te steunen in een separate beheeromgeving.

Oplossingen

Ivanti heeft updates uitgebracht om de kwetsbaarheden in Ivanti Endpoint Manager te verhelpen. Zie de referentie voor meer informatie.

Referenties

- <https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022>