



Advisory NCSC-2024-0236

Kwetsbaarheden verholpen in Ivanti Endpoint Manager

2024-06-14 Revisie 2

Updates

Revision: 0

Initiele versie

Revision: 1

Referentie toegevoegd

Revision: 2

Onderzoekers hebben Proof-of-Concept-code (PoC) gepubliceerd, waarmee de kwetsbaarheid met kenmerk CVE-2024-29824 kan worden aangetoond. Uitvoer van de PoC vereist kennis van de inrichting van het systeem en toegang tot de lokale infrastructuur waar het EPM is geïmplementeerd.

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.

Feiten

Ivanti heeft kwetsbaarheden verholpen in Endpoint Manager.

Interpretaties

Een kwaadwillende kan de kwetsbaarheden misbruiken om middels SQL Injection willekeurige code uit te voeren op het systeem.

Voor succesvol misbruik moet de kwaadwillende toegang hebben tot de lokale infrastructuur waar het EPM systeem is geïmplementeerd.

Onderzoekers hebben Proof-of-Concept-code gepubliceerd, waarmee de kwetsbaarheid met kenmerk CVE-2024-29824 kan worden aangetoond.

Oplossingen

Ivanti heeft updates uitgebracht om de kwetsbaarheden te verhelpen in Ivanti EPM 2022 SU5. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://forums.ivanti.com/s/article/KB-Security-Advisory-EPM-May-2024?language=en_US