Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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.

Uw reacties zijn welkom op info@ncsc.nl

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