Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0376

Kwetsbaarheden verholpen in Docker Desktop

2024-09-18 Revisie 0

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

Er zijn kwetsbaarheden verholpen in Docker Desktop.

Interpretaties

Een kwaadwillende kan de kwetsbaarheden misbruiken om willekeurige code uit te voeren in de context van de Desktop-applicatie. Omdat de Docker Desktop veelal door ontwikkelaars wordt gebruikt, is niet uit te sluiten dat de uitvoer van willekeurige code daarmee met verhoogde rechten kan plaatsvinden.

Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden een malafide extension te implementeren en gebruiken.

Oplossingen

De ontwikkelaars van Docker hebben updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://docs.docker.com/desktop/release-notes/#4342