



Advisory NCSC-2024-0318

Kwetsbaarheden verholpen in Docker Moby

2024-07-25 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.first.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 is een kwetsbaarheid verholpen in Docker Moby.

Interpretaties

De kwetsbaarheid stelt een kwaadwillende in staat om via een API request zijn rechten te verhogen door middel van het omzeilen van een beveiligingsmaatregel. Deze kwetsbaarheid is alleen te misbruiken als er gebruik wordt gemaakt van een AuthZ plugin om toegangsrechten te beheren.

Oplossingen

Het Docker team heeft een update uitgebracht om de kwetsbaarheid te verhelpen in Moby. Als updaten niet mogelijk is wordt door Docker geadviseerd om de plug-in uit te schakelen. Daarnaast is het goed gebruik om leastprivilege op een dergelijke API toe te passen.

Zie de referentie voor meer informatie.

Referenties

- <https://nvd.nist.gov/vuln/detail/CVE-2024-41110>
- <https://www.cve.org/CVERecord?id=CVE-2024-41110>
- <https://www.docker.com/blog/docker-security-advisory-docker-engine-authz-plugin/>