



Advisory NCSC-2025-0037

Kwetsbaarheden verholpen in VMware Aria Operations

2025-01-31 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

VMware heeft kwetsbaarheden verholpen in VMware Aria Operations.

Interpretaties

De kwetsbaarheden omvatten een informatielek dat kwaadwillenden met View Only Admin-rechten in staat stelt om mogelijk de inloggegevens van geïntegreerde VMware-producten te lezen. Daarnaast is er een opgeslagen cross-site scripting-kwetsbaarheid die niet-administratieve gebruikers in staat stelt om kwaadaardige scripts in te voegen, wat kan leiden tot ongeautoriseerde toegang en acties. Een privilege-escalatiekwetsbaarheid stelt kwaadwillenden met niet-administratieve rechten in staat om operaties uit te voeren als een admin-gebruiker. Bovendien kan een andere opgeslagen cross-site scripting-kwetsbaarheid door een administrator worden misbruikt tijdens een verwijderactie, wat de browser van het slachtoffer kan beïnvloeden. Tot slot kan een informatielek kwaadwillenden met niet-administratieve rechten in staat stellen om inloggegevens voor een uitgaande plugin te verkrijgen, mits zij een geldig service credential ID kennen.

Oplossingen

VMware heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25329>