Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0037

Kwetsbaarheden verholpen in VMware Aria Operations

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 31-01-2025

TLP:WHITE

Toegestane verspreiding van 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 van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

VMware heeft kwetsbaarheden verholpen in VMware Aria Operations.

Duiding

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

Kwetsbaarheden

CVE	CVSS Score
› CVE-2025-22218	8.5 HIGH
› CVE-2025-22219	6.8 MEDIUM
› CVE-2025-22220	4.3 MEDIUM
› CVE-2025-22221	5.2 MEDIUM
› CVE-2025-22222	7.7 HIGH

CWE's

CWE	Beschrijving
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor

Getroffen producten

vmware
aria_operations
aria_operations_for_logs
cloud_foundation
vmware_aria_operations
vmware_aria_operations_for_logs

Disclaimer