Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0449

Kwetsbaarheden verholpen in Adobe InDesign

2024-11-18 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

Adobe heeft kwetsbaarheden verholpen in InDesign desktop applicaties (Specifiek voor versies ID18.5.3, ID19.5 en eerder).

Interpretaties

De kwetsbaarheden bevinden zich in de manier waarop de InDesign desktop applicaties omgaan met speciaal vervaardigde bestanden. Dit kan leiden tot een heap-gebaseerde buffer overflow, wat een aanvaller in staat stelt om willekeurige code uit te voeren. Succesvol misbruik vereist gebruikersinteractie, aangezien de kwetsbaarheden alleen kan worden misbruikt door het openen van een kwaadwillig bestand. Dit verhoogt het risico op onbedoelde activatie door gebruikers, wat een bedreiging vormt voor de integriteit en vertrouwelijkheid van gegevens in de context van het slachtoffer.

Oplossingen

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

Referenties

- https://helpx.adobe.com//security/products/indesign/apsb24-88.html