



Advisory NCSC-2024-0351

Kwetsbaarheden verholpen in Google Chrome en Chromium

2024-08-22 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

Google heeft kwetsbaarheden verholpen in Chrome en Chromium.

Interpretaties

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service te veroorzaken of code uit te voeren in de browser van het slachtoffer en daarmee mogelijk toegang krijgen tot gevoelige gegevens in de context van de browser van het slachtoffer.

Google meldt berichten te hebben ontvangen dat de kwetsbaarheid met kenmerk CVE-2024-7971 beperkt en gericht wordt misbruikt. Publieke Proof-of-Concept-code (PoC) of een publieke exploit is (nog) niet beschikbaar.

Oplossingen

Google heeft updates uitgebracht om de kwetsbaarheden te verhelpen in Chrome en Chromium 128.0.6613.84 en 128.0.6613.85. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html