Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0427

Kwetsbaarheden verholpen in Google Chrome

2024-10-30 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

Google heeft kwetsbaarheden verholpen in Chrome.

Interpretaties

Een kwaadwillende kan de meest ernstige kwetsbaarheid (CVE-2024-10487) misbruiken om via een 'out-of-bounds write' willekeurige code uit te voeren op het systeem waarop de browser geinstalleerd staat. Hiervoor hoeft het slachtoffer alleen een besmette website of website met besmette advertentie te bezoeken.

Er is voor deze kwetsbaarheid momenteel geen actief misbruik of beschikbaarheid van PoC code bekend.

Oplossingen

Google heeft updates uitgebracht om de kwetsbaarheid te verhelpen in Chrome 130.0.6723.91 en 130.0.6723.92. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop_29.html
- https://issues.chromium.org/issues/375123371
- https://issues.chromium.org/issues/374310077