



NCSC-2026-0341

Kwetsbaarheden verholpen in Google Chrome

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 04-09-2026

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

Google heeft meerdere kwetsbaarheden verholpen in Google Chrome, specifiek in versies voor 152.0.7977.82.

Duiding

De kwetsbaarheden bevinden zich in verschillende componenten van Google Chrome, waaronder DevTools, Network, V8 JavaScript engine en Transactions Platform op iOS. Aanvallers kunnen deze kwetsbaarheden misbruiken door speciaal vervaardigde HTML-pagina's aan te bieden, wat kan leiden tot het uitvoeren van willekeurige code buiten de sandboxomgeving, het omzeilen van toegangsbeperkingen, het lezen van geheugen buiten de sandbox, en het compromitteren van de isolatie van webcontent. De kwetsbaarheden zijn specifiek van toepassing op Google Chrome en zijn verschillende componenten, inclusief versies op Android en iOS.

Google geeft aan dat voor CVE-2026-85046 publieke PoC beschikbaar is.

Oplossingen

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

Referenties

➤ https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-85042	9.6 CRITICAL
➤ CVE-2026-85043	
➤ CVE-2026-85044	
➤ CVE-2026-85045	7.5 HIGH
➤ CVE-2026-85046	8.8 HIGH
➤ CVE-2026-85047	9.6 CRITICAL
➤ CVE-2026-85048	8.3 HIGH

> CVE-2026-85049	8.8 HIGH
> CVE-2026-85050	9.6 CRITICAL
> CVE-2026-85052	3.1 LOW
> CVE-2026-85053	8.8 HIGH

CWE's

CWE	Beschrijving
> CWE-125	Out-of-bounds Read
> CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
> CWE-416	Use After Free
> CWE-459	Incomplete Cleanup
> CWE-672	Operation on a Resource after Expiration or Release
> CWE-787	Out-of-bounds Write
> CWE-825	Expired Pointer Dereference
> CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')

Getroffen producten

Google
Chrome

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.