Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0354

Kwetsbaarheid verholpen in Google Chrome

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-09-2026

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 een zeroday-kwetsbaarheid verholpen in de V8 JavaScript engine van Google Chrome.

Duiding

Google meldt dat de kwetsbaarheid met kenmerk CVE-2026-87491 actief wordt misbruikt. Het betreft een out-of-bounds write in de V8-engine van Google Chrome, die voorkomt in versies vóór 153.0.8010.36. Een kwaadwillende kan een speciaal vervaardigde HTML-pagina gebruiken om de kwetsbaarheid te activeren en binnen de sandbox willekeurige code uit te voeren. De kwetsbaarheid wordt veroorzaakt door onjuiste bounds checking in het geheugenbeheer van V8, wat kan leiden tot geheugenbeschadiging. Succesvol misbruik kan daarnaast leiden tot toegang tot gegevens buiten de toegewezen geheugenbuffer, waardoor gevoelige informatie kan worden buitgemaakt of de browser kan crashen.

Oplossingen

Google heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html
- https://issues.chromium.org/issues/543557673

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-87491	

CWE's

CWE	Beschrijving
CWE-787	Out-of-bounds Write

Getroffen producten

Google
Chrome

Disclaimer