



NCSC-2025-0142

Kwetsbaarheden verholpen in Mozilla Firefox en Thunderbird

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 06-05-2025

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

Mozilla heeft kwetsbaarheden verholpen in Firefox en Thunderbird (Specifiek voor versies onder 138 en 128.10).

Duiding

De kwetsbaarheden omvatten privilege-escalatie door code-injectie, onveilige verwerking van WebGL-shaderattributen, onjuiste isolatie van processen, en lokale code-executie door inadequate sanitatie van speciale karakters. Deze kwetsbaarheden kunnen leiden tot gevoelige informatielekken, geheugenbeschadiging en de mogelijkheid voor aanvallers om schadelijke commando's uit te voeren buiten de sandbox van de browser.

Oplossingen

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

Referenties

- <https://www.mozilla.org/security/advisories/mfsa2025-28/>
- <https://www.mozilla.org/en-us/security/advisories/cve-feed.json>
- <https://www.mozilla.org/security/advisories/mfsa2025-29/>
- <https://www.mozilla.org/en-us/security/advisories/cve-feed.json>
- <https://www.mozilla.org/security/advisories/mfsa2025-30/>
- <https://www.mozilla.org/en-us/security/advisories/cve-feed.json>
- <https://www.mozilla.org/security/advisories/mfsa2025-31/>
- <https://www.mozilla.org/en-us/security/advisories/cve-feed.json>
- <https://www.mozilla.org/security/advisories/mfsa2025-32/>
- <https://www.mozilla.org/en-us/security/advisories/cve-feed.json>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-2817	8.5 HIGH
➤ CVE-2025-4082	5.3 MEDIUM
➤ CVE-2025-4083	5.3 MEDIUM
➤ CVE-2025-4084	2.3 LOW

> CVE-2025-4085	5.1 MEDIUM
> CVE-2025-4086	5.3 MEDIUM
> CVE-2025-4087	5.3 MEDIUM
> CVE-2025-4088	5.3 MEDIUM
> CVE-2025-4089	2.3 LOW
> CVE-2025-4090	5.1 MEDIUM
> CVE-2025-4091	5.3 MEDIUM
> CVE-2025-4092	5.3 MEDIUM
> CVE-2025-4093	5.3 MEDIUM

CWE's

CWE	Beschrijving
> CWE-653	Improper Isolation or Compartmentalization
> CWE-138	Improper Neutralization of Special Elements
> CWE-1021	Improper Restriction of Rendered UI Layers or Frames
> CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
> CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
> CWE-532	Insertion of Sensitive Information into Log File
> CWE-451	User Interface (UI) Misrepresentation of Critical Information
> CWE-125	Out-of-bounds Read
> CWE-352	Cross-Site Request Forgery (CSRF)
> CWE-284	Improper Access Control
> CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
> CWE-94	Improper Control of Generation of Code ('Code Injection')

➤ CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
➤ CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
➤ CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Getroffen producten

Mozilla
Firefox
Firefox ESR
Thunderbird
Thunderbird ESR

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.