



NCSC-2025-0040

Kwetsbaarheden verholpen in Mozilla Firefox en Thunderbird

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 07-02-2025

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 135 en 128.7).

Duiding

De kwetsbaarheden omvatten onder andere een double-free kwetsbaarheid, use-after-free condities, en race conditions die kunnen leiden tot geheugenbeschadiging, ongeautoriseerde toegang, en privacyrisico's. Kwaadwillenden kunnen deze kwetsbaarheden misbruiken om willekeurige code uit te voeren, spoofing-aanvallen uit te voeren, en gevoelige gebruikersdata bloot te stellen.

Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden een malafide pagina te openen of link te volgen.

Oplossingen

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

Referenties

- <https://www.mozilla.org/security/advisories/mfsa2025-08/>
- <https://www.mozilla.org/en-us/security/advisories/cve-feed.json>
- <https://www.mozilla.org/security/advisories/mfsa2025-11/>
- <https://www.mozilla.org/en-us/security/advisories/cve-feed.json>
- <https://www.mozilla.org/security/advisories/mfsa2025-10/>
- <https://www.mozilla.org/en-us/security/advisories/cve-feed.json>
- <https://www.mozilla.org/security/advisories/mfsa2025-09/>
- <https://www.mozilla.org/en-us/security/advisories/cve-feed.json>
- <https://www.mozilla.org/security/advisories/mfsa2025-07/>
- <https://www.mozilla.org/en-us/security/advisories/cve-feed.json>

Kwetsbaarheden

| CVE | CVSS Score |
|----------------------------------|------------|
| ➤ CVE-2024-11704 | 6.9 MEDIUM |
| ➤ CVE-2025-0510 | 6.9 MEDIUM |

| | |
|-----------------|------------|
| > CVE-2025-1009 | 6.9 MEDIUM |
| > CVE-2025-1010 | 6.9 MEDIUM |
| > CVE-2025-1011 | 6.9 MEDIUM |
| > CVE-2025-1012 | 6.9 MEDIUM |
| > CVE-2025-1013 | 6.3 MEDIUM |
| > CVE-2025-1014 | 5.3 MEDIUM |
| > CVE-2025-1015 | 5.3 MEDIUM |
| > CVE-2025-1016 | 6.9 MEDIUM |
| > CVE-2025-1017 | 6.9 MEDIUM |
| > CVE-2025-1018 | 6.9 MEDIUM |
| > CVE-2025-1019 | 6.9 MEDIUM |
| > CVE-2025-1020 | 6.9 MEDIUM |

CWE's

| CWE | Beschrijving |
|------------|---|
| > CVE-1021 | Improper Restriction of Rendered UI Layers or Frames |
| > CVE-415 | Double Free |
| > CVE-362 | Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |
| > CVE-404 | Improper Resource Shutdown or Release |
| > CVE-119 | Improper Restriction of Operations within the Bounds of a Memory Buffer |
| > CVE-416 | Use After Free |
| > CVE-295 | Improper Certificate Validation |
| > CVE-79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |

Getroffen producten

| |
|----------------|
| mozilla |
| firefox_esr |
| firefox |
| thunderbird |

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.