



NCSC-2024-0425

Kwetsbaarheden verholpen in Mozilla Firefox en Thunderbird

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 30-10-2024

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.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Cross-Site-Scripting (XSS)
- Denial-of-Service (DoS)
- Toegang tot gevoelige gegevens

Oplossingen

Mozilla heeft updates uitgebracht om de kwetsbaarheden te verhelpen in Firefox en Thunderbird 132, Thunderbird 128.4, Firefox ESR 115.17 en 128.4. Voor meer informatie, zie bijgevoegde referenties.

Referenties

- <https://www.mozilla.org/en-US/security/advisories/mfsa2024-59/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2024-58/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2024-57/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2024-56/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2024-55/>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-10458	8.2 HIGH
➤ CVE-2024-10459	7.6 HIGH
➤ CVE-2024-10460	4.3 MEDIUM
➤ CVE-2024-10461	6.1 MEDIUM
➤ CVE-2024-10462	7.5 HIGH
➤ CVE-2024-10463	7.5 HIGH

> CVE-2024-10464	7.5 HIGH
> CVE-2024-10465	7.5 HIGH
> CVE-2024-10466	7.5 HIGH
> CVE-2024-10467	9.8 CRITICAL
> CVE-2024-10468	9.8 CRITICAL

CWE's

CWE	Beschrijving
> CVE-799	Improper Control of Interaction Frequency
> CVE-280	Improper Handling of Insufficient Permissions or Privileges
> CVE-942	Permissive Cross-domain Policy with Untrusted Domains
> CVE-203	Observable Discrepancy
> CVE-290	Authentication Bypass by Spoofing
> CVE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
> CVE-125	Out-of-bounds Read
> CVE-416	Use After Free
> CVE-400	Uncontrolled Resource Consumption
> CVE-770	Allocation of Resources Without Limits or Throttling
> CVE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
> CVE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
> CVE-20	Improper Input Validation
> CVE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

mozilla
firefox
firefox_esr
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.