Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0016

Kwetsbaarheden verholpen in Mozilla Firefox en Thunderbird

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 15-01-2025

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 134 en 128.6).

Duiding

De kwetsbaarheden omvatten onder andere client-side path traversal, privilege escalation en use-after-free condities. Deze kwetsbaarheden kunnen door kwaadwillenden worden misbruikt om ongeautoriseerde toegang te verkrijgen, crashes te veroorzaken of mogelijkerwijze willekeurige code uit te voeren.

Oplossingen

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

Referenties

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-06/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-05/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-04/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-03/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-02/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-01/

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-50336	
CVE-2025-0237	6.8 MEDIUM
CVE-2025-0238	6.5 MEDIUM
CVE-2025-0239	5.4 MEDIUM
CVE-2025-0240	6.5 MEDIUM
CVE-2025-0241	

CVE-2025-0242	8.8 HIGH
CVE-2025-0243	7.5 HIGH
CVE-2025-0244	8.1 HIGH
CVE-2025-0245	
CVE-2025-0246	6.5 MEDIUM
CVE-2025-0247	9.8 CRITICAL
CVE-2025-23108	
CVE-2025-23109	6.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-441	Unintended Proxy or Intermediary ('Confused Deputy')
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-451	User Interface (UI) Misrepresentation of Critical Information
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-416	Use After Free
CWE-295	Improper Certificate Validation
CWE-863	Incorrect Authorization
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-787	Out-of-bounds Write
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-20	Improper Input Validation
CWE-346	Origin Validation Error

CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

mozilla
firefox
firefox_esr
firefox_for_ios
thunderbird
thunderbird_esr

Disclaimer