



.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Vulnérabilité affectant le navigateur Mozilla Firefox
Numéro de Référence	54250205/25
Date de publication	02 Mai 2025
Risque	Important
Impact	Important

Systèmes affectés

- Mozilla Firefox versions antérieures à 138
- Mozilla Firefox ESR versions antérieures 128.10
- Mozilla Firefox ESR versions antérieures 115.23

Identificateurs externes

CVE-2025-2817	CVE-2025-2817	CVE-2025-2817	CVE-2025-2817	CVE-2025-4082
CVE-2025-4082	CVE-2025-4082	CVE-2025-4082	CVE-2025-4083	CVE-2025-4083
CVE-2025-4083	CVE-2025-4083	CVE-2025-4084	CVE-2025-4084	CVE-2025-4085
CVE-2025-4085	CVE-2025-4086	CVE-2025-4086	CVE-2025-4087	CVE-2025-4087
CVE-2025-4087	CVE-2025-4088	CVE-2025-4088	CVE-2025-4089	CVE-2025-4089
CVE-2025-4090	CVE-2025-4090	CVE-2025-4091	CVE-2025-4091	CVE-2025-4091
CVE-2025-4092	CVE-2025-4092	CVE-2025-4093		

Bilan de la vulnérabilité

Mozilla Foundation annonce la disponibilité d'une mise à jour de sécurité permettant la correction de plusieurs vulnérabilités au niveau du navigateur Mozilla Firefox. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire, d'accéder à des données confidentielles ou d'élever ses privilèges.

Solution

Veillez se référer au bulletin de sécurité Mozilla afin d'installer les nouvelles mises à jour.

Risques

- Exécution de code arbitraire à distance
- Accès à des données confidentielles
- Elévation de privilèges

Références

Bulletins de sécurité Mozilla:

- <https://www.mozilla.org/en-US/security/advisories/mfsa2025-28/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2025-29/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2025-30/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2025-31/>