



WebGL shader attribute memory corruption in Thunderbird for macOS

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2025-4082
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-29 14:15:34 UTC
Updated	2026-04-13 15:16:59 UTC
Description	Modification of specific WebGL shader attributes could trigger an out-of-bounds read, which, when chained with other vulne

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from ADP

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Problem Types: CWE-125 | CWE-125 CWE-125 Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown	
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	None

Availability

None

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N



NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mozilla	Firefox	unaffected 115.23 115.* rpm	Not specified
CNA	Mozilla	Firefox	unaffected 128.10 128.* rpm	Not specified
CNA	Mozilla	Firefox	unaffected 138 * rpm	Not specified
CNA	Mozilla	Thunderbird	unaffected 128.10 128.* rpm	Not specified
CNA	Mozilla	Thunderbird	unaffected 138 * rpm	Not specified

References

Reference	Source	Link	Tags
bugzilla.mozilla.org/show_bug.cgi	security@mozilla.org	bugzilla.mozilla.org	Permission
www.mozilla.org/security/advisories/mfsa2025-32	security@mozilla.org	www.mozilla.org	Vendor Ad
www.mozilla.org/security/advisories/mfsa2025-31	security@mozilla.org	www.mozilla.org	Vendor Ad
www.mozilla.org/security/advisories/mfsa2025-30	security@mozilla.org	www.mozilla.org	Vendor Ad
lists.debian.org/debian-lts-announce/2025/05/msg00022.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	
www.mozilla.org/security/advisories/mfsa2025-28	security@mozilla.org	www.mozilla.org	Vendor Ad
www.mozilla.org/security/advisories/mfsa2025-29	security@mozilla.org	www.mozilla.org	Vendor Ad
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,



Vendor Comments And Credit

Discovery Credit

CNA: un3xploitable & GF (en)

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)