



# Information disclosure due to uninitialized memory in the Graphics: Canvas2D component

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-6749
<b>State</b>	PUBLISHED
<b>Assigner</b>	mozilla
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-21 13:16:20 UTC
<b>Updated</b>	2026-04-22 14:52:10 UTC
<b>Description</b>	Information disclosure due to uninitialized memory in the Graphics: Canvas2D component. This vulnerability was fixed in Fi

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from ADP

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

**EPSS:** 0.000360000 probability, percentile 0.105350000 (date 2026-04-22)

**Problem Types:** CWE-908 | CWE-908 CWE-908 Use of Uninitialized Resource

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/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 115.35 115.* rpm	Not specified
CNA	Mozilla	Firefox	unaffected 140.10 140.* rpm	Not specified
CNA	Mozilla	Firefox	unaffected 150 * rpm	Not specified
CNA	Mozilla	Thunderbird	unaffected 140.10 140.* rpm	Not specified
CNA	Mozilla	Thunderbird	unaffected 150 * rpm	Not specified

#### References

Reference	Source	Link	Tags
bugzilla.mozilla.org/show_bug.cgi	security@mozilla.org	bugzilla.mozilla.org	Permissions Required
www.mozilla.org/security/advisories/mfsa2026-34	security@mozilla.org	www.mozilla.org	Vendor Advisory
www.mozilla.org/security/advisories/mfsa2026-30	security@mozilla.org	www.mozilla.org	Vendor Advisory
www.mozilla.org/security/advisories/mfsa2026-31	security@mozilla.org	www.mozilla.org	Vendor Advisory
www.mozilla.org/security/advisories/mfsa2026-32	security@mozilla.org	www.mozilla.org	Vendor Advisory
www.mozilla.org/security/advisories/mfsa2026-33	security@mozilla.org	www.mozilla.org	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

#### Vendor Comments And Credit

Discovery Credit

**CNA:** Inseo An (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](#)