

CVE-2025-62593

Ray-Project Ray Code Injection Vulnerability

CISA KEV since Aug 17, 2026

Actively exploited

Ray is an AI compute engine. Prior to version 2.52.0, developers working with Ray as a development tool can be exploited via a critical RCE vulnerability exploitable via Firefox and Safari. This vulnerability is due to an insufficient guard against browser-based attacks, as the current defense uses the User-Agent header starting with the string "Mozilla" as a defense mechanism. This defense is insufficient as the fetch specification allows the User-Agent header to be modified.

EVRS 81/100 Urgent priority	CVSS V4.0 9.4 Critical · NVD	EPSS 0.625 99.19th percentile · FIRST	CISA DEADLINE Aug 20, 2026 CISA federal deadline · Overdue by 2 months
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☒ KEV recency	Added to CISA KEV within the last 90 days
☒ EPSS	0.625 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.4	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.
Basis: CISA KEV required action

Combined with a DNS rebinding attack against the browser, and this vulnerability is exploitable against a developer running Ray who inadvertently visits a malicious website, or is served a malicious advertisement (malvertising). This issue has been patched in version 2.52.0.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
ray	< 2.52.0	2.52.0	GitHub

Sources

Vendor guidance	github.com/advisories/GHSA-q279-jhrf-cc6v	github.com	github.com/ray-project/ray/security/advisories/GHSA-q279-jhrf-cc6v
github.com	github.com/ray-project/ray/commit/70e7c72780bdec075dba6cad1afe0832772bfe09	BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk
Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk	NVD	nvd.nist.gov/vuln/detail/CVE-2025-62593
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-199754
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-62593		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.