EXPLOITED VULNERABILITY ADVISORY: CVE-2025-62593

Summary

CVE-2025-62593 in Ray-Project Ray is being actively exploited in the wild. 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. 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. CISA requires federal remediation by 2026-08-20; under the CRA, exploitation of an affected product must be reported within 24 hours.

What we know

- **CVE:** CVE-2025-62593
- **Affected:** Ray-Project Ray
- **Exploitation:** Actively exploited, added to CISA KEV on 2026-08-17
- **Severity:** CVSS 8.8 High, Network-exploitable, no privileges required (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
- **Exploitation likelihood (EPSS):** 0%
- **Weakness:** CWE-94, CWE-352

Recommended action

Patch CVE-2025-62593 by 2026-08-20. If you cannot patch immediately, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. If you ship an affected product, be ready to file the CRA 24-hour report the moment you find it exploited.

Sources: CISA Known Exploited Vulnerabilities, NIST NVD. Public data; an advisory of active exploitation, not an incident report. Verify applicability to your estate before acting.