NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-63106

Summary

CVE-2026-63106 is a newly disclosed Critical vulnerability. It is not yet on CISA's actively-exploited list; treat it as proactive patching before it is weaponised. ReadyEcommerce before 4.5.2 contains an unauthenticated SQL injection vulnerability in the product listing API where the rating parameter from the products endpoint is concatenated directly into a MySQL HAVING clause without parameterization in ProductController.php. Attackers can perform time-based blind SQL injection through the unsanitized rating parameter to extract the full database contents, including user credentials and administrator password hashes, with potential additional file system access due to the database connection running as root.

What we know

- **CVE:** CVE-2026-63106
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.8 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. This does not yet trigger CRA 24-hour reporting, which requires active exploitation, but patching ahead of exploitation is the whole point.

Sources: NIST NVD. Public data; an advisory of a newly disclosed vulnerability, not an incident report. Verify applicability to your estate before acting.