

NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-53791

Summary

CVE-2026-53791 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. rsync daemon before 3.5.0 contains an IP address spoofing vulnerability that allows unauthenticated remote attackers to bypass IP-based access controls by sending a crafted PROXY protocol header with a forged source address. Attackers who can connect directly to the rsync daemon can inject a spoofed source IP in the PROXY protocol header to circumvent hosts allow/deny rules, gaining unauthorized access that would otherwise be blocked based on their real source address.

What we know

- **CVE:** CVE-2026-53791
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.1 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:N)

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.