Nextcloud CVE-2026-110447 ? 60-Minute Runbook

Exploited in the wild

Fixed by: richdocumentscode 26.4.303 or higher ? or remove the app

Unauthenticated remote code execution through the "Collabora Online - Built-in CODE Server" app (richdocumentscode) whenever its document server is not running. Web shells have been found planted on real servers since September 2026.

Minutes 0-5 ? Confirm your version

1. SSH into the Nextcloud server and run: sudo -u www-data php occ app:list | grep richdocumentscode
2. Below 26.4.303 -> you are EXPOSED. Continue this runbook now.
3. 26.4.303 or higher -> patched for this CVE; skip to the minute 50-60 verification block and finish early.

Minutes 5-15 ? Snapshot before you touch anything

1. Take a VM/filesystem snapshot or backup of the Nextcloud directory and database so a compromise hunt can compare against a known point in time.
2. Note the current app version and the time you started ? you will need both for the log hunt below.

Minutes 15-30 ? Patch: update or remove the app

1. Update the "Collabora Online - Built-in CODE Server" app to 26.4.303 or higher, or remove the app entirely.
2. Disabling the app does NOT protect you ? update or remove, nothing else counts.
3. Standalone Collabora servers (not the built-in app) are not affected by this CVE.

Minutes 30-50 ? Hunt for signs of past compromise

1. Search web logs for hits to the vulnerable endpoint around any restart or upgrade window: grep "proxy.php" /var/log/apache2/access.log | grep -v " 200 "
2. Look for PHP files you did not put there inside your Nextcloud directories ? three admins found web shells this way before the CVE was published.
3. If you were vulnerable during Sept-Oct 2026, assume you need to look: an exposed window plus a web shell means treating the host as compromised, not just patched.

Minutes 50-60 ? Verify and document

1. Re-run the version check from minutes 0-5 and confirm 26.4.303+ (or that the app is gone).
2. Record: version before, version after, log-hunt result, and the time the patch landed. If you found a web shell, stop here and start incident response ? do not just delete it.
3. Re-check in 7 days: repeat the log grep for proxy.php hits.

Source: Fleet checker: nextcloud-cve-2026-110447.html (advisory Oct 14, 2026)

Generated by BreachHunter (Ingenious AI) from the fleet’s published exposure checker for this CVE. Assessment guidance only ? verify eac