

Threat actors exploit critical Collabora RCE flaw to backdoor Nextcloud servers



Attackers are exploiting CVE-2026-110447, a critical command execution vulnerability in Nextcloud's Collabora app, to deploy webshells and search for credentials since mid-September.

- CVE-2026-110447 affects Collabora Online Built-in CODE Server app versions before 26.4.303 for Nextcloud
- Active exploitation began in mid-September, more than four weeks before CVE publication on October 14
- Attackers deploy PHP webshells to search for password databases, password managers and cryptocurrency wallets
- The flaw requires no authentication and exploits a command injection in the proxy.php endpoint when the server is stopped

- A 33-day gap between the September 11 patch and CVE publication hampered administrator response

Vulnerability details and exploitation timeline

Threat actors are actively exploiting **CVE-2026-110447**, a critical remote code execution vulnerability in the Collabora Online Built-in CODE Server app for Nextcloud. The flaw affects versions before 26.4.303 and resides in the app's mechanism for starting the bundled Collabora server. Exploitation began in mid-September, with administrator reports documenting attacks as early as September 10.

The vulnerability allows attackers to inject operating system commands through the app's proxy.php endpoint without requiring authentication or user interaction. A key prerequisite is that the built-in CODE server must be stopped, such as after a restart, upgrade or crash. The flaw affects only the optional built-in CODE server app; standalone Collabora Online servers, Docker and package-based installations, and Nextcloud All-in-One deployments remain unaffected.

Attack patterns and delayed disclosure

Administrators reported that attackers deployed PHP webshells and used them to search for password databases, password manager artifacts and cryptocurrency wallets. The vendor committed a fix on September 9 and released version 26.4.303 on September 11, but the formal advisory and CVE were not published until October 14, creating a gap of more than four weeks. A community warning was issued on October 3 urging immediate updates due to ongoing exploitation, but the absence of a CVE identifier made it difficult for administrators to assess the issue and implement defenses.

Broader implications for vulnerability management

Research from Second Security found that the median interval between public fixes and CVE publication rose to 39 days in August, up from 5.1 days in January. The researchers attribute this to growing volumes of AI-assisted vulnerability discoveries straining CVE processing systems. In many cases, public exploit code appeared within hours of security fixes and days before CVE publication, with AI tools enabling attackers to generate working exploits rapidly from published patches.

What to do now

1. Immediately upgrade Collabora Online Built-in CODE Server app (richdocumentscode) to version 26.4.303 or later on all Nextcloud instances
2. Remove the built-in CODE server app entirely if it is not required for business operations; disabling alone is insufficient
3. Conduct forensic review of all Nextcloud servers running affected versions for PHP webshells, particularly in web-accessible directories

4. Search system logs for suspicious requests to proxy.php endpoints dating back to September 10
5. Review access logs for evidence of credential harvesting, password database queries or cryptocurrency wallet searches
6. Implement compensating controls to monitor and alert on command execution attempts in web application directories until patching is complete