

CVE-2026-110447

Collabora Online – Built-in CODE Server OS Command Injection Vulnerability

Exigent

CISA KEV since Oct 23, 2026

Actively exploited

Collabora Online Built-in CODE Server before 26.4.303 (richdocumentscode), a Nextcloud app, allows remote code execution, as exploited in the wild in September and October 2026, a different vulnerability than CVE-2025-66208. This is an OS command injection in proxy.php when the CODE server isn't running (e.g., the product was recently restarted). The vulnerability is not present in standalone Collabora Online servers; only this deployment with CODE Server is affected.

EVRS 85/100 Immediate priority	CVSS V4.0 9.2 Critical · NVD	EPSS 0.123 96.2nd percentile · FIRST	CISA DEADLINE Oct 26, 2026 CISA federal deadline in 0 days
--	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☒ KEV recency	Added to CISA KEV within the last 30 days
☒ EPSS	0.123 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
Collabora / Collabora Online – Built-in CODE Server	–	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-f97p-r72q-64h2	Additional guidance	help.nextcloud.com/t/to-collabora-built-in-user-update-asap/250516
github.com	github.com/CollaboraOnline/online/security/advisories/GHSA-g3vx-3m76-fghh	BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk
Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk	NVD	nvd.nist.gov/vuln/detail/CVE-2026-110447
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-100780
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-110447		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.