



OS CCK 8.3.16 for Joomla Fixes a No-Login PHP Upload and an SQL Injection, but the Updater Still Offers 8.3.14

OS CCK for Joomla before 8.3.16 let anyone upload and run PHP (CVE-2026-102427, CVSS 10.0) and had a no-login SQL injection. The updater won't offer the fix.

Phil E. Taylor | 30 September 2026

OrdaSoft has released OS CCK 8.3.16, and it fixes two security flaws in the Joomla extension, both reachable with no login. The worse one is CVE-2026-102427, which the Joomla CNA scores at the maximum CVSS 10.0: any visitor could upload a file to a site running OS CCK below 8.3.16 and have the server run it as PHP. The other is an SQL injection in the public listing pages, fixed in the same release with no CVE and no advisory.

The bigger problem is that neither fix will reach most of the sites that need it. OrdaSoft's own update server still tells Joomla that the current version is the older, vulnerable 8.3.14, so no affected site is offered 8.3.16. It has to be installed by hand.

How mySites.guru flags OS CCK on your Joomla sites

mySites.guru records the exact version of every extension on every connected Joomla site in each snapshot, twice a day. We added both flaws to our Joomla vulnerability database, CVE-2026-102427 the same afternoon its record was published, so any site running OS CCK below 8.3.16 now shows them on its site card and in its audit, with 8.3.16 as the version that resolves them. The flag works from the installed version, so it does not rely on Joomla's updater, which is the part that is broken here.

The Pro edition installs under the same element, `com_os_cck`, but numbers its versions differently from the free Light line. A Pro install inside the affected range is flagged. OrdaSoft publishes no Pro changelog, so we cannot tell you which Pro build includes the fixes, and we would rather flag it than guess it safe.

How the OS CCK upload handler let anyone write PHP to a Joomla site

OS CCK lets site owners build custom content types, and those types can have image fields that visitors fill in from the front end. The upload behind those fields is a file called `site/uploader.php`, reached through the component's normal routing with

`task=getContent` . The dispatcher just includes the file. There is no login check and no permission check anywhere on that path, so the request works from an anonymous browser.

The handler did try to make sure the upload was an image. It read the file's first bytes with `mime_content_type()` and compared the result against the image types in OS CCK's own MIME table. That is a real content check, better than trusting the browser's `Content-Type` header. The problem was the other half. According to the CVE record, the list of allowed file extensions was in the source but commented out, and the saved file's extension came straight from the filename the attacker sent.

10.0
CVSS 4.0

CRITICAL Joomla CNA · [CVE-2026-102427](#)

Anyone can upload a PHP file and run it, with no account on the site.

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

No login needed

Single request

▼ [What does this mean?](#)

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

How it is reached

AV:N Network: Reachable across the internet

AC:L Low: Nothing to work around, it just works

AT:N None: Works against any affected install

PR:N None: No account needed

UI:N None: Nobody has to be tricked into anything

What it does to the site

VC:H High: Everything the site holds can be read

VI:H High: Data and files can be altered at will

VA:H High: The site can be taken down

What it does beyond the site

SC:H High: Data on other systems can be read

SI:H High: Other systems can be altered

SA:H High: Other systems can be taken down

Put those two facts together and you have the exploit. A polyglot file, one that opens with real GIF or PNG header bytes and has PHP source appended after them, satisfies the content check because its first bytes really are an image. Saved as `shell.php`, it then goes into a folder under the site's `images` directory, and PHP executes anything ending in `.php` in that folder when a browser asks for it. The CNA's own summary names that exact technique.

A malicious actor's own code runs on your server, with the same access as the website itself: reading, changing or deleting any file it can touch, planting a backdoor that survives the next update, installing malware, pulling every database credential and API key from your configuration, and using your server to attack other people. Gulp.

What OrdaSoft changed in the OS CCK 8.3.16 upload handler

We read the 8.3.16 Light package. The upload handler now defines an extension allow-list of `jpg`, `jpeg`, `png`, `gif` and `webp`, and rejects any upload whose lower-cased extension is not on it before the file is saved. The magic-byte check is still there, so an upload now has to pass both: look like an image, and be named like one. That pairing is what the [OWASP file upload guidance](#) asks for, because each check alone has a known bypass.

One thing did not change. In 8.3.16 the `getContent` task is still reached with no login and no permission check, and uploads still go to `images/com_os_cck<n>/original/` under the web root. That is by design for a front-end form, and with the allow-list back in place it no longer gives an attacker code execution. It does mean anonymous visitors can still put image files on the server, which is relevant if disk space or content moderation is a concern on the site.

The second flaw: a no-login SQL injection in record sorting

A content construction kit exists to show lists of things, and a list needs to be sortable. OS CCK takes the name of the sort column from the request and uses it to build the **ORDER BY** clause of the query behind the listing. In the releases before 8.3.16 that value went into the query through a filter whose real job is a keyword blacklist, not a column allow-list, which is not enough to stop an **ORDER BY** injection.

In 8.3.16 the listing code compares the requested sort field against the actual columns of the content type, plus a short list of known sort keys, and falls back to a safe default when it matches none of them. The previous, unrestricted line is still in the file, commented out, one line above its replacement. That is the same fix OrdaSoft shipped days earlier for three other extensions that did get CVEs.

The SQL injection has no CVE

CVE-2026-102427 covers the upload flaw only. The sort-order SQL injection has no record, no severity score and no advisory, so trackers keyed on CVE identifiers will not show it. The change is in the code OrdaSoft shipped, and that is enough to act on. Updating to 8.3.16 fixes both.

Why the fix will not reach most Joomla sites

Joomla extensions update through an update server: the vendor publishes a small XML manifest that names the current version and links to the download, and every site checks it. OrdaSoft's OS CCK manifest still names version **8.3.14**.

Joomla's updater compares the version in that manifest against the version installed on the site. A site already on 8.3.14 or 8.3.15 is therefore told it is up to date, and 8.3.16 is never offered, even though the download link inside that same manifest now serves the fixed 8.3.16 file. The patch is sitting on OrdaSoft's server, wired to the update system,

and labelled as older than it is. Only a site that happens to be on something below 8.3.14, or an owner who reinstalls by hand, ends up on the fixed release.

So the fix shipped, and the update system that is supposed to deliver it will not. That gap, between a patch existing and a patch arriving, is the reason a version flag across a whole portfolio beats trusting each vendor's updater to do its job.

Why a content check alone is not enough for Joomla extension uploads

Checking the bytes of an upload answers one question: does the start of this file look like an image? It says nothing about what the server will do with the file once it is saved. On almost every Joomla host, that decision comes from the file's extension. A `.php` file under the web root goes to PHP, whatever its first bytes are. PHP ignores leading binary junk and runs the first `<?php` block it finds.

So the extension is the control that decides whether an upload becomes code, and the content check is a second layer on top. Commenting out the allow-list removed the layer that mattered. OS CCK is the fifth OrdaSoft extension to get a security fix in September after [OS Gallery](#) and the Real Estate Manager, Vehicle Manager and Book Library batch, and [CVE-2026-102427](#) credits the same researcher, Ala Arfaoui. OS Gallery's worst finding was also an upload that trusted the attacker's filename.

A web server rule that blocks PHP execution inside `images` would have stopped this class of flaw on any site that had one. Joomla does not ship that rule by default, and most hosts do not add it.

Why a sort parameter keeps becoming an SQL injection in Joomla extensions

Escaping and parameter binding protect a value, the kind of thing that sits inside quotes in a query, like a search term or an ID. They work by making sure an attacker cannot break out of those quotes. A column name in an `ORDER BY` clause is part of the

query's structure instead: it sits there with no quotes around it, and a prepared statement cannot bind it. There is no quote to escape, so whatever the attacker sends is read as SQL from the first character. A filter that strips or blacklists a few keywords does not change that.

The fix is always the same, and it is the one OS CCK 8.3.16 now applies: compare the requested sort column against a fixed allow-list of the columns the listing is allowed to sort by, and fall back to a default when it matches none. Joomla's own list models do exactly this with their `filter_fields` allow-list. The sort direction gets the same treatment, reduced to `ASC` or `DESC` and nothing else.

How rare is OS CCK across the sites we monitor?

Rarely used. Only a handful of connected sites in the mySites.guru database run OS CCK at all. That is good news for Joomla sites in general and bad news for the few that run it, because a rarely used extension with no advisory and a broken update path gets little attention. No mailing list will warn its owners, and the Joomla updater tells them they are up to date.

Is CVE-2026-102427 being exploited?

There is no public report of exploitation yet. The CVE is not on CISA's Known Exploited Vulnerabilities catalogue, and CISA's assessment attached to the record says exploitation none, automatable yes, technical impact total. The record's own `E:A` (attacked) value is the Joomla CNA's default on every record it publishes, so it should not be read as evidence either way.

Automatable is the part to take seriously. The attack is a single unauthenticated POST to a predictable URL, with a file anyone can build in a text editor. It needs no human in the loop, which is the kind of flaw mass scanners add once a record is public.



Find PHP files hiding in the images folder

mySites.guru checks every connected site for this automatically and flags it the moment it appears. It runs as part of the full audit on every connected Joomla site.

Check your site for free →

What to do if you run OS CCK on a Joomla site

1. Install 8.3.16 or later by hand. Download the current package from ordasoft.com, install it over the top in the Joomla extension manager, and check the installed version afterwards. Do not wait for the updater.
2. If you cannot update today, disable the component in the extension manager. Unpublishing a menu item does not help, because the upload task and the listing pages answer on the component's own URL.
3. Search the **images** folder, and especially any **images/com_os_cck*/original/** folders, for **.php**, **.phtml** or **.phar** files. Nothing in a Joomla images folder should be code. If you find one, treat the site as compromised and work through our [Joomla hacked-site guide](#).
4. Treat the database as potentially read on any site that sat on an affected version: check the Super User and Administrator groups for accounts your team did not create, reset Super User passwords, and rotate the Joomla secret and any API keys or mail credentials stored on the site.

Find Super User accounts you did not create

mySites.guru checks every connected site for this automatically and flags it the moment it appears. It runs as part of the full audit on every connected site.

Check your site for free →

If a site is already showing signs of a break-in and you would rather hand it over, [we can fix it for you](#). If you manage Joomla sites for clients, the [free audit](#) shows what mySites.guru finds on your own sites first, and a [subscription](#) keeps every connected site checked against flaws like these the day they are published, whether or not the vendor's updater is working.

Timeline

2026-09-20



The OrdaSoft wave starts with OS Gallery

The Joomla CNA publishes four CVEs against OrdaSoft's OS Gallery, including an unauthenticated SQL injection, all fixed in 6.2.7 with no vendor advisory.

2026-09-28



Three more OrdaSoft extensions get six CVEs

Real Estate Manager, Vehicle Manager and Book Library each get an unauthenticated SQL injection in their listing sort order, plus a reflected XSS. Same finder, same class of flaw.

2026-09-29



OrdaSoft releases OS CCK 8.3.16

The 8.3.16 Light package restores the upload handler's file-extension allow-list and rewrites the listing sort handling to validate the sort column. There is no advisory.

2026-09-30



The Joomla CNA publishes [CVE-2026-102427](#)

The record covers the upload flaw, scores it CVSS 4.0 10.0 Critical and credits Ala Arfaoui. OrdaSoft's update stream still advertises 8.3.14, and mySites.guru flags every connected site running OS CCK below 8.3.16.

Further Reading

- [CVE-2026-102427 on mySites.guru](#) - the record, the affected range and the CVSS breakdown.
- [Three OrdaSoft Joomla extensions have unauthenticated SQL injections in their sort order](#) - the six-CVE batch the OS CCK SQL injection fix belongs to.
- [OS Gallery 6.2.7 fixes an unauthenticated SQL injection and two authenticated RCEs](#) - where the OrdaSoft wave started.
- [OWASP File Upload Cheat Sheet](#) - why an extension allow-list and a content check are two separate controls, and you need both.
- [OWASP SQL Injection Prevention Cheat Sheet](#) - see its section on allow-list validation for table and column names.
- [OrdaSoft OS CCK product page](#) - where the 8.3.16 download lives.

Frequently Asked Questions

What is CVE-2026-102427?

An unauthenticated remote code execution flaw in OrdaSoft's OS CCK, a content construction kit extension for Joomla. Its front-end upload handler accepts a file from anyone, keeps the extension from the attacker's filename, and saves it where PHP will run it. The Joomla CNA scores it CVSS 4.0 10.0 Critical. It is fixed in 8.3.16.

Which versions of OS CCK are affected?

The CVE record lists versions 1.0.0 to 8.3.15 for the upload flaw, and the SQL injection fix is also in 8.3.16, so anything below 8.3.16 should be updated. The Pro edition installs under the same Joomla element, `com_os_cck`, and numbers its versions differently, so a Pro install is flagged too. OrdaSoft publishes nothing that confirms the Pro edition's fixed version.

Does either flaw need a login?

No. The upload flaw's CVSS vector says PR:N, and the code agrees: the upload is reached through OS CCK's ordinary front-end routing as `task=getContent`, and nothing on that path checks who the visitor is. The SQL injection sits on the public record-listing pages any visitor can open.

Is there a CVE for the OS CCK SQL injection?

Not for the SQL injection. [CVE-2026-102427](#) covers the upload flaw only. The evidence for the SQL injection is the 8.3.16 release itself: its front-end listing code now validates the sort column against real column names, with the old, unrestricted line left commented out directly above the new check. OrdaSoft applied the same fix to Real Estate Manager, Vehicle Manager and Book Library, which do have CVEs.

Will Joomla's update system offer me OS CCK 8.3.16?

No. OrdaSoft's update manifest at [ordasoft.com](#) still advertises 8.3.14. Joomla's updater compares that number against your installed version, so a site on 8.3.14 or 8.3.15 is told it is up to date and is never offered 8.3.16, even though the download behind that manifest is the fixed file. Download and reinstall it by hand.

Is OS CCK being exploited in the wild?

There is no public report of it. [CVE-2026-102427](#) is not on CISA's Known Exploited Vulnerabilities list, and CISA's assessment on the record says exploitation none,

automatable yes, technical impact total. With a flaw this simple to automate, that can change quickly.

How do I check whether a site was already compromised?

Look for any .php file under the site's images folder, especially in folders named com_os_cck followed by a number, and check the Super User group for accounts you did not create. mySites.guru's audit flags PHP files inside /images on every connected Joomla site.

Is OS CCK a widely used Joomla extension?

No. It is rarely used, and only a handful of connected sites in the mySites.guru database run it at all. That is why a fix with no advisory and a broken update path is dangerous for the sites that do: no one is going to tell them to act.

AI MODIFIED

Written and edited by a human, with AI assistance. [Our approach to AI](#)

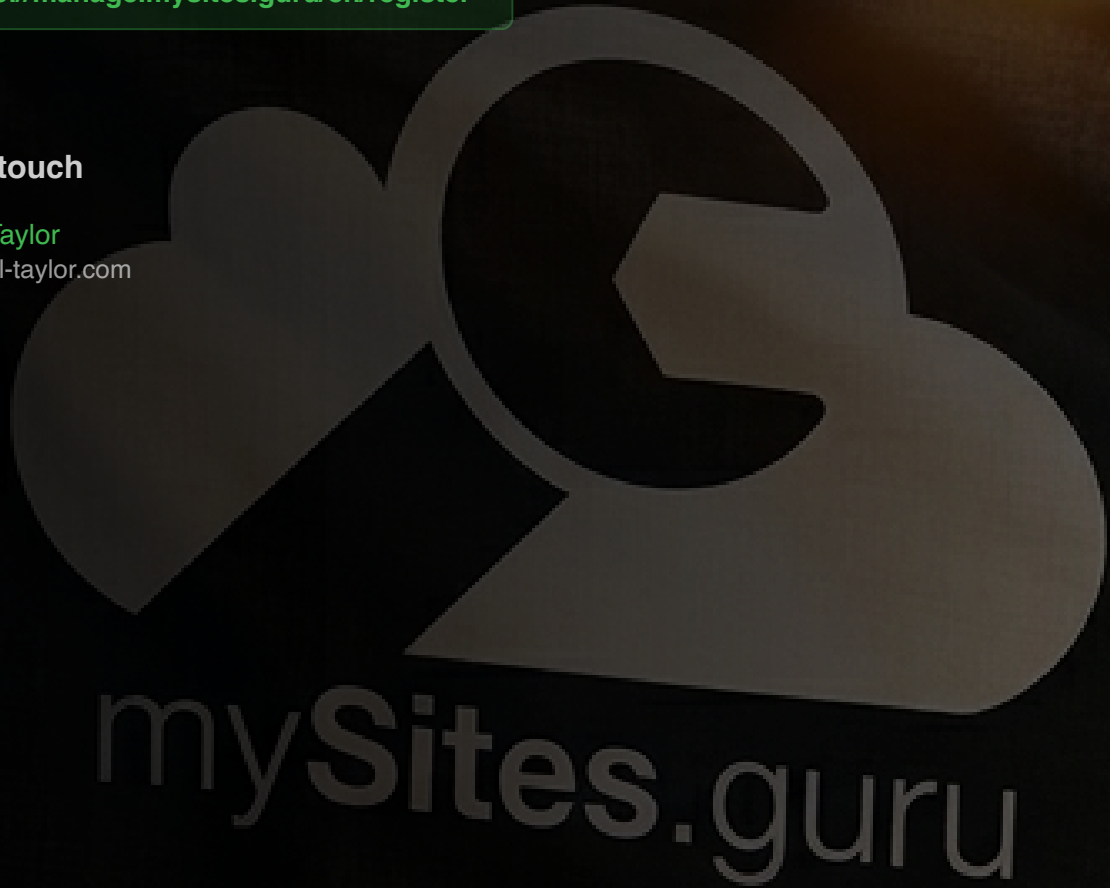
Get Your Free Site Audit

See how your WordPress and Joomla sites measure up.
No credit card required.

<https://manage.mysites.guru/en/register>

Get in touch

Phil E. Taylor
phil@phil-taylor.com



© 2026 Blue Flame Digital Solutions Limited. All rights reserved.

mysites.guru

