mySites.guru

OS Gallery 6.2.7 Fixes an Unauthenticated SQL Injection and Two Authenticated RCEs

OrdaSoft's OS Gallery below 6.2.7 has an SQL injection needing no login, two routes to remote code execution, and a second SQL injection. Update now.

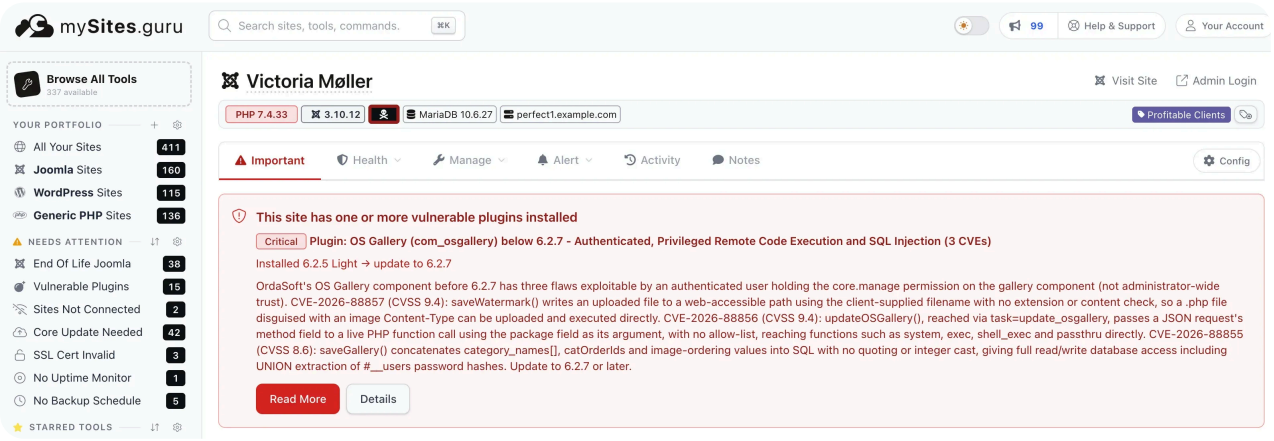
Phil E. Taylor | 20 September 2026

OrdaSoft's OS Gallery, a gallery extension for Joomla, has four new vulnerabilities published today by the Joomla CNA, and between them they cover the two attacker starting points that matter most in any CMS extension: an unauthenticated route straight into the database, and two separate routes from an ordinary gallery-manager account to running code on the server. If you manage a Joomla site with OS Gallery installed on any version up to 6.2.6, it needs updating regardless of who logs in or how the gallery is used.

The four split into two groups: one needs no login at all, and three need an account holding a specific permission on the gallery component. Which group a flaw falls into changes how urgently it matters to you.

How mySites.guru flags this automatically

You do not need to read the rest of this post to find out whether you are affected. mySites.guru's extension inventory tracks OS Gallery's installed version on every connected Joomla site, and any site on 6.2.6 or below, Light edition included, is already flagged on its own site card, no searching required. If you manage sites outside mySites.guru too, the breakdown below tells you what to check for.



Two ways from a gallery-manager account to running code on the server

The highest CVSS score of the four is a tie: CVE-2026-88857 and CVE-2026-88856 both score 9.4 Critical, and both need an account holding core.manage on the OS Gallery component, the permission Joomla grants to a gallery manager rather than a site administrator.

CVE-2026-88857 is a file upload flaw in `saveWatermark()`. The function copies an uploaded file into a web-accessible directory using the filename exactly as the client sent it, with no check on the file's extension and no check on its actual content, only the Content-Type header the client claims. A gallery manager, or an attacker who has taken over one, can name the upload `shell.php`, set the Content-Type to `image/jpeg`, and the server stores it under its real name and later runs it when requested directly.

9.4
CVSS 4.0

CRITICAL Joomla CNA · CVE-2026-88857

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

CVE-2026-88856 does not even need a file upload. The `updateOSGallery()` function, reached through `task=update_osgallery`, reads a JSON request body and takes the value of a `method` field, then calls it as a live PHP function using a `package` field from the same request as its argument. There is no allow-list of permitted function names, so anything callable with one argument is reachable, including `system`, `exec`, `shell_exec` and `passthru`.

9.4
CVSS 4.0

CRITICAL Joomla CNA · CVE-2026-88856

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

Either one gives an attacker who already holds gallery-manager access the same shell your hosting provider has.

The search box needs no login at all

One step down by CVSS, and the only one of the four that needs no account whatsoever, is CVE-2026-88854. OS Gallery's front-end search, delivered through the `mod_osgallery_search` module that ships with the extension, reads the `textsearch` and `searchText` request parameters with Joomla's `getVar()`, which despite the name is not one of Joomla's real input filters and does not touch quotes or SQL syntax, only HTML tags. The value goes straight into a `LIKE` clause with no escaping.

9.3 CVSS 4.0

CRITICAL Joomla CNA · CVE-2026-88854

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

`mod_osgallery_search` is the kind of module that ends up on a page and gets forgotten about: a small search box next to a gallery, doing what a search box does. Anyone who can reach that page, which is anyone who can reach the site, can send a crafted search term and pull data straight out of the database with a UNION SELECT, administrator password hashes included. No login, no CSRF token, no gallery-manager account required.

A second SQL injection at the same permission level

The fourth CVE, CVE-2026-88855, scores lowest of the four at 8.6 High. `saveGallery()` passes form data through a hand-rolled parser into Joomla's Input object, then reads it back with filter types that do not sanitise SQL content. Values from `category_names[]`, `catOrderIds` and the image-ordering fields go straight into SQL with no quoting and no integer cast, and an account with core.manage on the gallery can use it to read and write the whole database, including a UNION-based pull of the `#__users` password hashes.

8.6
CVSS 4.0

HIGH Joomla CNA · CVE-2026-88855

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

Who found this, and what OrdaSoft has said

All four CVEs credit the same finder, Ala Arfaoui, a security researcher whose public disclosure history up to now is entirely WordPress: more than a dozen credited CVEs, mostly cross-site request forgery and SQL injection in smaller WordPress plugins, going back several years. As far as the CVE records show, these four OS Gallery findings are the first time that work has crossed over into Joomla.

OrdaSoft's own site has no changelog entry, no security page and no mention of any of the four CVE numbers as of publication. We could not find a public advisory, a release announcement, or any acknowledgement of the finder. The only place 6.2.7 is named as the fix is inside the four CVE records themselves. That is not unusual for a small extension vendor, most of the vendor self-fixes we cover here say considerably more than this, but it does mean the version number in this post is the only public confirmation of the fix available right now.

OS Gallery does not currently appear on the Joomla Vulnerable Extensions List, and these four CVEs are the first ever published against `com_osgallery`. There is no earlier history to compare the fix against.

How to check every OS Gallery site you manage

By hand, checking one site means logging in, opening the extension manager, filtering for OS Gallery, reading the version, and updating anything on 6.2.6 or below. On one site that is a few minutes. Across forty sites it is most of an afternoon, and it is the kind of afternoon where site thirty-one gets less attention than site three.

In mySites.guru, search the extension inventory once for OS Gallery and get back every connected site running it with its current version, and any site below 6.2.7 is flagged on its own site card without you searching for anything.

If a gallery-manager account on any of your sites was compromised through either RCE route, the practical next step is finding whatever was left behind. A planted PHP file does not have to look like a webshell to behave like one.

What the numbers look like across the sites we manage

As of today, the large majority of the OS Gallery installs we can see across the Joomla sites on mySites.guru are on a version below 6.2.7, which is what you would expect on the day four new CVEs are published against an extension that had none before. That is not a criticism of anyone running it. A fix released today has not had time to reach anyone, which is why we flag affected sites and email their owners rather than assuming a CVE record alone gets the word out.

OS Gallery ships a free “Light” edition alongside the paid one, and a site running it reports a version string like “6.2.5 Light” rather than a bare number. mySites.guru’s matcher strips the edition tag before comparing, so a Light install is judged on its version number the same way a Pro one is.

Timeline

2026-09-10 — **The four CVE identifiers are reserved**

The Joomla CNA reserves CVE-2026-88854 through CVE-2026-88857 for OS Gallery, ten days before any record is published.

2026-09-20 — **All four CVEs are published**

The Joomla CNA publishes all four records the same day, crediting Ala Arfaoui as the finder of all four. This is the extension's first published CVE history; no earlier CVE exists against com_osgallery.

2026-09-20 — **OS Gallery 6.2.7 is named as the fix**

All four published records name 6.2.7 as the version that resolves the flaw described in it. We could not find a public vendor advisory or changelog entry announcing the release independently of the CVE records.

2026-09-20 — **mySites.guru flags every affected site**

The detection rule covering OS Gallery 1.0.0 to 6.2.6 goes live, and every connected site running an affected version is flagged automatically on its site card.

Further Reading

- CVE-2026-88857 record - the file upload RCE, CWE-434.
- CVE-2026-88856 record - the arbitrary function call RCE, CWE-94.
- CVE-2026-88855 record - the authenticated SQL injection, CWE-89.
- CVE-2026-88854 record - the unauthenticated SQL injection, CWE-89.
- OWASP SQL Injection Prevention Cheat Sheet - the developer reference for parameterised queries.

- OWASP File Upload Cheat Sheet - why an upload endpoint needs its own content and permission checks.
- A month of Joomla security disclosures - the wider run of Joomla extension flaws this sits alongside.

Frequently Asked Questions

Which OS Gallery versions are affected by these four CVEs?

Every version from 1.0.0 up to and including 6.2.6, across all four CVEs (CVE-2026-88854, CVE-2026-88855, CVE-2026-88856 and CVE-2026-88857). The fix is OS Gallery 6.2.7. These are the first CVEs ever published against this extension, so there is no earlier affected range to compare against.

What can an anonymous visitor actually do with CVE-2026-88854?

OS Gallery's front-end search box passes what a visitor types straight into a database query with no escaping. Anyone at all, with no account and no login, can use it to extract data from the site's database, including administrator password hashes and session data. This is the only one of the four that needs no authentication at all.

What can a gallery-manager account do with the other three?

An account holding core.manage permission on the OS Gallery component, which Joomla calls a gallery manager rather than an administrator, can reach all three remaining flaws. CVE-2026-88857 disguises an uploaded PHP file as an image and runs it directly. CVE-2026-88856 sends a JSON request naming a PHP function and an argument, and the code calls that function with no allow-list, reaching functions like system and shell_exec. CVE-2026-88855 is a second SQL injection, requiring the same manager account.

Does this affect Joomla itself?

No. OS Gallery is a third-party gallery extension from OrdaSoft, not part of Joomla core. A Joomla site without OS Gallery installed is not affected by any of these four CVEs. The Joomla CNA assigns CVE identifiers for third-party Joomla extensions as well as for core, which is why these look like Joomla CVEs at a glance.

What about Joomla 3 sites? Is there a separate fix?

There is no separate branch to worry about. Some Joomla extensions maintain one version line for Joomla 3 and a different, incompatible one for Joomla 4 and above, which means a single version rule misses half the affected sites. OS Gallery is not built that way: it uses one continuous version scheme across Joomla 3, 4, 5 and 6, and we can see Joomla 3 sites already running 6.2.5 and 6.2.6 in the wild. A Joomla 3 site can install 6.2.7 the same way any other site does.

How do I find every OS Gallery site I manage?

By hand, you would need to log in to each Joomla site and check its installed extensions one at a time. mySites.guru searches the extension inventory once and returns every connected site running OS Gallery with its version, and flags any site on 6.2.6 or below automatically, without you checking each site by hand.

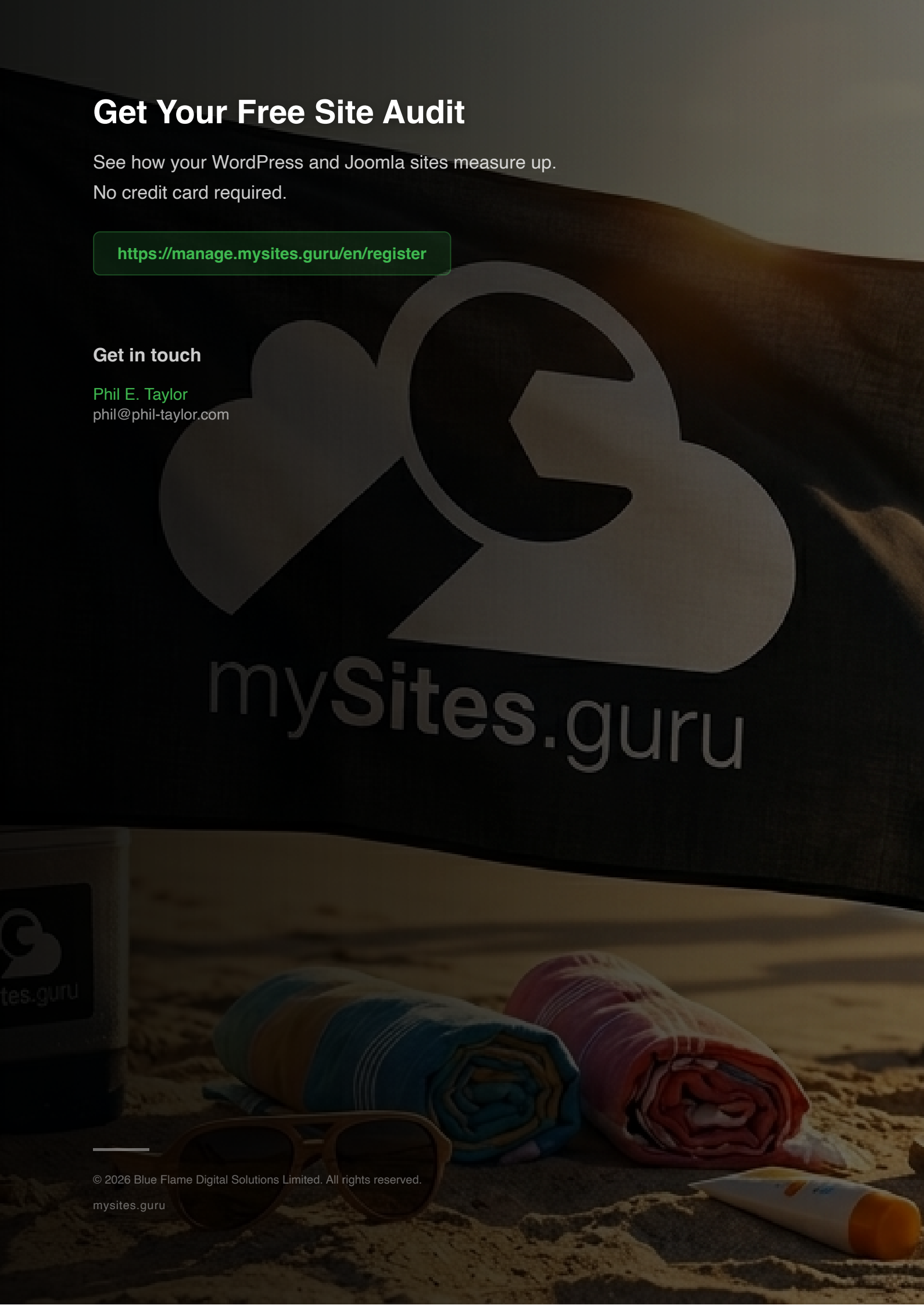
Written and edited by a human, with AI assistance. Our approach to AI

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