



Phoca Gallery 6.1.6 fixes a stored XSS hidden in a photo's EXIF data

Phoca Gallery 4.5.0 to 6.1.5 lets a crafted image's EXIF data run script on the photo info view. 6.1.6 fixes it on Joomla 6 only; Joomla 4 and 5 are stranded.

Phil E. Taylor | 23 October 2026

On 19 October 2026 Phoca released Phoca Gallery 6.1.6, a security release for the Joomla gallery extension. The release notes say one thing about it: "This is a security release." The Joomla CNA published the detail as CVE-2026-102786 on 23 October 2026, a stored cross-site scripting flaw through HTML attribute injection, affecting Phoca Gallery 4.5.0 to 6.1.5.

We read the 6.1.5 to 6.1.6 diff to work out what that means for a site running the extension. It means a photo can attack the person looking at it. The EXIF metadata inside an uploaded image was written into the photo's info page without escaping, so a crafted image runs script in the browser of anyone who opens that view, and the fix is only on offer to Joomla 6 sites.

TL;DR

- Phoca Gallery **4.5.0 to 6.1.5** builds the front-end photo info view from the image's own EXIF metadata, and raw fragments of it reach the page markup
- A crafted EXIF value **breaks out of an HTML attribute** and runs as script when anyone opens that photo's info view, in the context of your site
- The attacker needs to get an image into a gallery: back-end upload rights, or the front-end user upload feature, which is **off by default**
- **6.1.6 fixes it**, and only on the Joomla 6 line. The current Joomla 5 (5.1.3) and Joomla 4 (4.5.5) releases are inside the affected range with no patched successor
- Most affected sites run Joomla 6 and update normally. Joomla 4 and 5 sites have to install the 6.x package by hand or remove the component
- The flaw is CVE-2026-102786, CVSS 4.0 8.6 High, published by the Joomla CNA on 23 October 2026. This is Phoca's fix; we analysed the release after it shipped

8.6

CVE-2026-102786 CVE-2026-102786: stored XSS through a gallery image's EXIF data

CVSS 4.0

HIGH

Joomla CNA

A crafted image's EXIF metadata runs script in the browser of anyone who opens that photo's info view, in the context of your site. That can hijack a logged-in session, including an administrator's.

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

Needs gallery upload access

Fires on the photo info view

Fix only on the Joomla 6 line

▼ 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:A Active: Someone has to be talked through a few steps

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:L Low: The site slows or stutters

What it does beyond the site

SC:N None: Other systems keep their data

SI:N None: Other systems keep their integrity

SA:N None: Other systems stay up

How a photo's EXIF data becomes script in Phoca Gallery

Phoca Gallery has a front-end info view for each image that shows the camera data stored inside the file: the EXIF block that a camera or phone writes at capture time, and that any image editor can rewrite afterwards. Part of that block is the GPS position, which EXIF stores as fractions, and the view in `site/views/info/view.html.php` split those fractions on the `/` and joined the pieces into a display string for the page.

Before 6.1.6 the pieces went into that string exactly as they were read from the file. The view expected numbers and never checked that it had them. An EXIF field that holds a quote mark and some markup instead of a number closes the HTML attribute it was dropped into, and whatever follows is parsed as part of the page. The browser runs it with the site's own origin, for whoever opened the photo.

That is what makes this stored rather than reflected. The payload lives in the image file in the gallery, so it fires for every visitor who opens that photo's info view until the image is removed, with nothing in the URL to give it away. An administrator who opens it from the back end hands over their session, which is why the CNA scored confidentiality and integrity both high.

The attacker's only requirement is to get the image into a gallery. On a typical site that means an account with upload rights in the Phoca Gallery back end. If the front-end user upload feature is switched on, which it is not by default, a lower-privileged user can do it from the public side. That is the gap between the CNA's title, which says "authenticated", and its vector, which says no privileges required: the person who plants the image needs access, the person it fires on needs none.

What changed in Phoca Gallery 6.1.6

The fix is in one file, the info view, and it is the only functional change between the 6.1.5 and 6.1.6 tags. Each component of the EXIF fractions is now cast to a float before it is used, and a division by zero is guarded so a zero denominator no longer produces an error or an odd value. Only numeric data reaches the markup, so there is nothing left for a crafted EXIF value to break out with.

That is a narrow fix for a narrow path. It treats the GPS fields as numbers, which they are supposed to be, and it closes the attribute injection. It does not add output escaping across the rest of the view, so the release tells you which values were the problem rather than hardening the whole page, and the CNA's description matches that scope.

What we did and did not test

This is a reading of the released code, not an attack on anyone’s gallery. We have not uploaded an image to any live site, and we are not publishing a crafted file or a working EXIF value.

Which Phoca Gallery versions are affected?

Phoca Gallery 4.5.0 to 6.1.5 inclusive, which is the range the Joomla CNA record names. Phoca maintains one release line per Joomla version, and only the Joomla 6 line received the fix:

Joomla version	Newest Phoca Gallery the updater offers	Has the EXIF XSS fix?
Joomla 6	6.1.6	Yes
Joomla 5	5.1.3	No
Joomla 4	4.5.5	No
Joomla 3	3.2.8	Outside the published range (4.5.0 and up)

That table comes from [Phoca’s update manifest](#), which matches each Joomla generation to a release on a `targetplatform` pattern. The Joomla 5 release, 5.1.3, and the Joomla 4 release, 4.5.5, both sit inside 4.5.0 to 6.1.5 and neither has a patched successor. A site on either of them cannot update to safety from Joomla’s update screen.

The Joomla 3 line is a different case. Its newest release, 3.2.8, is below the 4.5.0 floor of the published range, so we are not claiming it is affected, and we are not claiming it is clean either. The CNA record does not cover it.

Joomla 4 and 5 sites have to install Phoca Gallery 6.1.6 by hand

Phoca's update feed offers each Joomla version one release, and Joomla discards any offered version that is not higher than the one installed. On Joomla 4 and Joomla 5 that produces two different failures:

- **A Joomla 4 or 5 site on the 4.x or 5.x line** is offered 4.5.5 or 5.1.3. Both are inside the affected range, so the site owner can apply the update in good faith and still be exposed.
- **A Joomla 4 or 5 site already running a 6.x build** is offered a lower version. Joomla shows no update at all, and the site looks current while it runs 6.1.5 or older.

The fix in both cases is the 6.x package from the [6.1.6 release](#), installed through Joomla's extension installer after a backup. That may mean moving the site to Joomla 6 first, and if the gallery is no longer earning its place on the site, removing the component is the shorter route.

Across the Joomla sites we manage, the majority of the affected Phoca Gallery installs run Joomla 6 and will update normally. About one in seven is on a Joomla 4 or 5 line with no fixed release. That proportion is from sites that an agency actively looks after; the wider Joomla world still runs a lot of Joomla 4, so the share of stranded galleries out there is likely higher.

An empty update list is not proof you are patched

On Joomla 4 and Joomla 5, Phoca Gallery can show no available update while running a vulnerable version, or offer an update that is itself inside the affected range. Check the installed version under System, Manage, Extensions and compare it with 6.1.6 by eye.

What to do about it on each Joomla version

1. **Joomla 6:** update Phoca Gallery to 6.1.6 through the normal Joomla updater, then confirm the version number.
2. **Joomla 5:** take a backup, then install the 6.x package by hand from the [GitHub release](#). Do not take the 5.1.3 the updater offers as a fix for this. If the package will not install on your site, plan the move to Joomla 6 or remove the gallery.
3. **Joomla 4:** the same choice. The updater's 4.5.5 is inside the affected range. Install the 6.x package by hand after a backup, which will usually mean moving the site to Joomla 6 first, or remove the component until you can.
4. **On any Joomla version:** this is stored XSS, so the question is who could have planted an image. If front-end user upload was ever enabled, review which accounts had it and what they uploaded. Check the existing galleries for images added by accounts you do not recognise, and treat an administrator who opened a suspect photo's info view as having a session that may have been used.

See which of your sites are still on Joomla 4 or 5

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 →

How mySites.guru flags vulnerable Phoca Gallery installs

The Phoca Gallery version alone does not tell you what to do here. You need the Joomla version beside it, because that decides whether the updater will deliver 6.1.6, whether you need the package by hand, or whether the site has to move to Joomla 6 first.

mySites.guru keeps both for each connected Joomla site. We added this flaw to our [vulnerability database](#) on the day the CVE was published, so every site running Phoca

Gallery between 4.5.0 and 6.1.5 is flagged on its dashboard now, with the Joomla version on the same screen. The Joomla 6 sites can go out in one batch with the mass updater, which leaves a short list of Joomla 4 and 5 sites for the manual package. That works the same way across a portfolio of Joomla sites of any size, and is part of every subscription.

Why a gallery's EXIF data is attacker-controlled

EXIF is written by whoever made the file. A camera fills it in, but so does any image editor, any command-line tool, and any script, and the file does not care whether the GPS field holds a fraction or a sentence. From the moment a site accepts an uploaded image, every byte of its metadata is input from the person who uploaded it, and a feature that reads that metadata back onto a page is an injection surface in the same way a comment form is. Developers tend to see the image as a blob and the EXIF as trusted camera data, when it is a user-supplied text block that happens to travel inside a JPEG.

In fifteen years of looking after client sites, the galleries have been the features nobody reviews. They are installed once for a photo page, the upload accounts are handed out to whoever runs the events, and the extension sits there for a decade. A flaw in the info view of a gallery on a site like that fires on the one person who clicks every photo to check it, which is usually the administrator.

This is the third Phoca extension this year where the fix reached only the current Joomla line. The Phoca Cart product filter SQL injection in August showed the distribution problem first, the Phoca Cart download IDOR in October repeated it, and the Phoca Download upload flaw had the same shape. Phoca is quick with the fix each time. What a site on an older Joomla gets from each release is a version number that looks current and the same vulnerable code underneath, and the release notes do not say which lines were left out.

Further Reading

- [CVE-2026-102786 at NVD](#) - the NVD record for the Phoca Gallery EXIF stored XSS.
- [CVE-2026-102786 on cve.org](#) - the Joomla CNA record with the affected range and the CVSS 4.0 vector.
- [Phoca Gallery 6.1.6 on GitHub](#) - the security release, with the package download for a manual install.
- [Phoca Gallery update manifest](#) - the feed that decides which Phoca Gallery each Joomla version is offered.
- [CWE-79: Improper Neutralization of Input During Web Page Generation](#) - the weakness class the CNA assigned.
- [OWASP Cross Site Scripting Prevention Cheat Sheet](#) - why data inside an HTML attribute needs its own escaping rules.

Frequently Asked Questions

What did Phoca Gallery 6.1.6 fix?

A stored cross-site scripting flaw in the front-end photo info view. Before 6.1.6 the view built its EXIF display from the raw metadata inside the image file, so a crafted EXIF value could break out of an HTML attribute and run script in the browser of anyone who opened that photo's info page. 6.1.6 casts the EXIF numeric fields to numbers before they reach the page.

Do I need to be logged in to exploit the Phoca Gallery EXIF flaw?

You need to get an image into a gallery, which on most sites means a back-end account with gallery upload rights, or the front-end user upload feature, which is off by default. The Joomla CNA record scores it with no privileges required but titles it authenticated; the honest reading is that the attacker needs upload access and the victim needs only to open the photo's info view.

Which Phoca Gallery versions are affected?

4.5.0 to 6.1.5 inclusive, according to the Joomla CNA record. That range includes the current releases on the Joomla 5 line (5.1.3) and the Joomla 4 line (4.5.5). Only 6.1.6, on the Joomla 6 line, has the fix.

Why does my Joomla 4 or Joomla 5 site not offer the Phoca Gallery 6.1.6 update?

Phoca's update feed offers one release per Joomla generation: 6.1.6 to Joomla 6, 5.1.3 to Joomla 5 and 4.5.5 to Joomla 4. The Joomla 5 and Joomla 4 releases are inside the affected range and have no patched successor, so the updater cannot deliver the fix on those sites. Install the 6.x package by hand, which may mean moving the site to Joomla 6 first, or remove the component.

Is there a CVE for the Phoca Gallery 6.1.6 fix?

Yes. The Joomla CNA published [CVE-2026-102786](#) on 23 October 2026 and scores it CVSS 4.0 8.6 High. The record names it an authenticated stored cross-site scripting through HTML attribute injection in Phoca Gallery 4.5.0 to 6.1.5.

Can mySites.guru tell me which of my sites run a vulnerable Phoca Gallery?

Yes. mySites.guru flags every connected Joomla site running Phoca Gallery between 4.5.0 and 6.1.5 on its dashboard, with the Joomla version beside it, which is what you need to

know whether the updater will offer the fix or you have to install it by hand.

AI MODIFIED

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

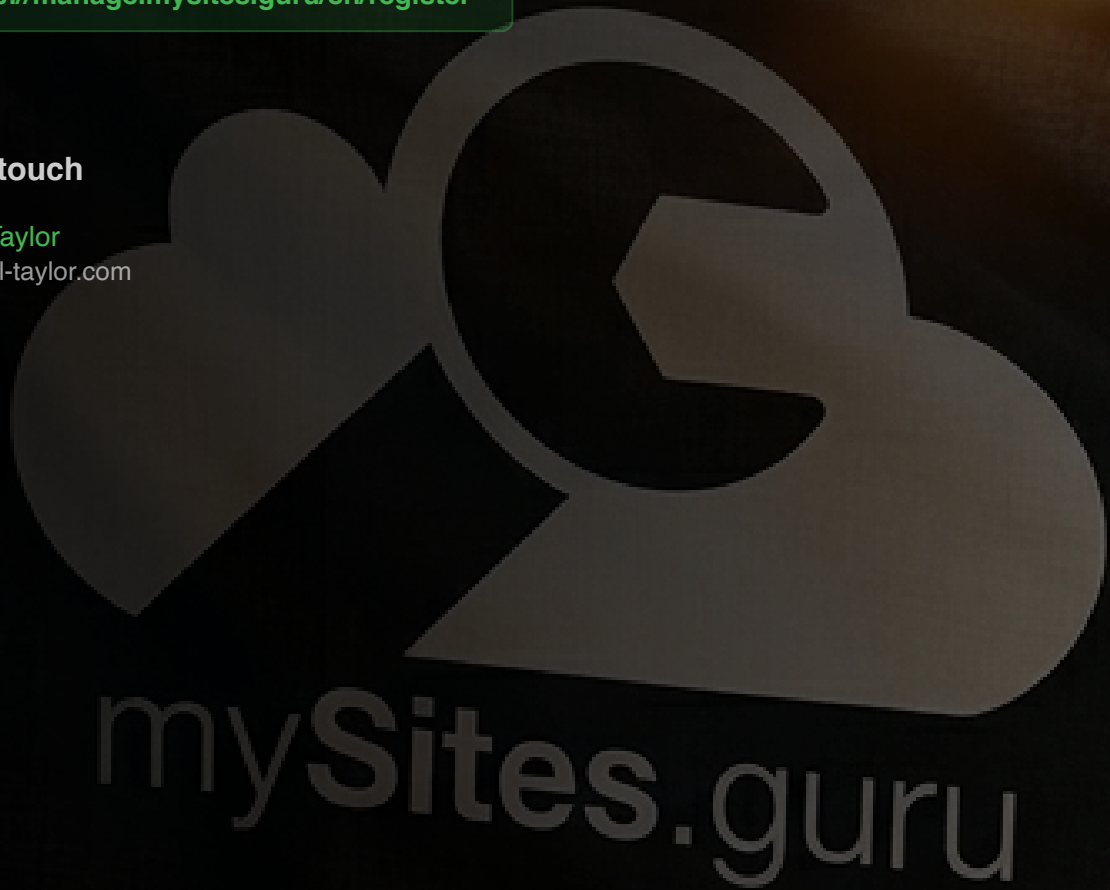
Get Your Free Site Audit

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