



Phoca Download 6.1.6 adds the token check its file delete was missing

Phoca Download 6.1.6 adds the missing CSRF token check to front-end publish, unpublish and delete. Low severity, but the fix exists only on the Joomla 6 line.

Phil E. Taylor | 26 October 2026

On 26 October 2026 Phoca released Phoca Download 6.1.6, a security release for the Joomla download-manager extension. The GitHub release says one thing: "This is a security release." Phoca's news post the same day adds a one-line changelog, "Security fix: Cross-Site Request Forgery", and says more details will be available in the CVE record. No CVE record has been published as of 26 October 2026.

We compared the 6.1.5 and 6.1.6 packages, and the fix is in one file: the front-end controller behind the User Control Panel's publish, unpublish and delete buttons, which now checks Joomla's anti-CSRF form token before it does anything. On its own this is a low severity flaw, and we score it that way below. What makes it worth a post is where the fix went. Only the Joomla 6 line received it, and across the sites we manage roughly seven in ten affected installs cannot get it from Joomla's update screen.

TL;DR

- Phoca Download's front-end User Control Panel has **publish, unpublish and delete** actions for files, in `site/controllers/user.php`
- Before 6.1.6 those tasks checked that the logged-in user held the category's **delete right**, but did not check Joomla's **form token**, so a crafted page or link could make that user's browser send the request, even as a plain GET
- Exposure needs a category's **Delete Rights** to be granted to front-end users, which is **closed by default**. No confidentiality impact, no code execution
- **6.1.6 fixes it** by routing all three tasks through one handler that calls `$this->checkToken( 'request' )` first
- The fix is on the **Joomla 6 line only**. Joomla 3, 4 and 5 are offered 3.2.3, 4.0.9 and 5.1.3, none of which checks the token
- About **seven in ten** affected installs we see cannot get 6.1.6 from the Joomla update screen
- We score it **2.3 Low** on CVSS 4.0. This is Phoca's fix; we analysed the release after it came out

2.3

CVSS 4.0

Phoca Download 6.1.6: cross-site request forgery on front-end file actions (no CVE yet)

LOW

mySites.guru assessment

A logged-in user who holds Delete Rights on a Phoca Download category, and who loads a page or link crafted by an attacker, has their browser publish, unpublish or delete a file in that category as them. Delete removes the file's database record, statistics and tag links, and the file itself if the component is set to delete existing files. Nothing is read and no code runs.

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

Needs a user with Delete Rights

Victim must be logged in

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:P Present: Needs a particular deployment or race to line up

PR:N None: No account needed

UI:P Passive: Someone has to visit a page

What it does to the site

VC:N None: Nothing can be read

VI:L Low: Some data can be altered

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 the Phoca Download file actions could be triggered from another site

Cross-site request forgery starts in the browser. When you are logged in to a Joomla site, your browser attaches your session cookie to every request it sends to that site, whether you typed the address, clicked a button on the site, or loaded a page somewhere else that happened to point at it. The site sees your cookie and treats the request as yours. Joomla's defence is the form token: a secret value written into each form that the server checks on submit, which a page on another site cannot know. Any action that changes something is supposed to require it.

Phoca Download's front-end User Control Panel lets a logged-in user manage files in the categories they have rights over, with publish, unpublish and delete actions handled by `site/controllers/user.php`. In 6.1.5 each of those three tasks asked one question: does this user hold the delete right on the file's category? If so, the task ran. The form token was never checked.

That gap means an attacker did not need the user's password, only their browser. A page or link built by the attacker, loaded by a logged-in user who holds the delete right, makes that user's browser send the publish, unpublish or delete request, and the site performs it as that user. Because no token was required, a plain GET request was enough: an image tag on a page the user happens to view will do it, with nothing to click.

What the attacker gets is limited. Delete removes the file's database record, its download statistics and its tag links. If the component option "Delete Existing Files" is set to Yes (the default is No), it also removes the file from the server's disk. Publish and unpublish change whether a file is visible. There is no way to read anything and no way to run code, which is why this scores Low.

Exposure also depends on a setting. The tasks reject any user who does not hold the delete right, and that right is granted per category through the "Delete Rights" option, which is closed by default. A site that has not opened Delete Rights to a front-end user or group on any category is not exposed, however many files it serves.

What changed in Phoca Download 6.1.6

The only code change between 6.1.5 and 6.1.6 is `site/controllers/user.php`. The three separate tasks now go through one shared handler, and its first line is `$this->checkToken('request')`. A request that arrives without a valid Joomla form token is rejected before the delete right is even looked at. The rest of the release is a version bump and refreshed help-page links.

A real user pressing the real buttons sees no difference. The User Control Panel form already submitted the token, and 6.1.6 makes the server require it.

What we did and did not test

This is a reading of the released code, not an attack on anyone's site. We have not sent a request to any live Phoca Download install, and we are not publishing a working request or proof of concept.

Which Phoca Download versions are affected?

Every Phoca Download release line below 6.1.6 lacks the token check on these tasks. Phoca keeps one release line per Joomla generation, and its update manifest decides which one each Joomla version is offered. Only the Joomla 6 line received the fix:

Joomla version	Phoca Download the updater offers	Has the token check?
Joomla 6	6.1.6	Yes
Joomla 5	5.1.3	No
Joomla 4	4.0.9	No
Joomla 3	3.2.3	No

We extracted 2.1.9, 3.2.3, 4.0.9, 5.1.3 and 6.0.0 and read the same controller in each. None of them checks the token on the publish, unpublish or delete tasks. So the Joomla 3, 4 and 5 lines are left without a fix: each is offered a version that is itself unprotected, with no fixed release behind it.

Seven in ten affected Phoca Download sites cannot update from the Joomla update screen

Two things combine here. The first is the table above: three of the four lines have no fixed release. The second is how Joomla's updater behaves when the manifest offers a version lower than the one installed. It discards it. A Joomla 5 site that already runs a 6.x build of Phoca Download is offered 5.1.3, which is lower, so the site shows no update at all and looks current while it runs the vulnerable code.

Across the Joomla sites connected to mySites.guru that run a vulnerable Phoca Download, as of 26 October 2026:

- About **30%** are Joomla 6 sites on the 6.x line. These get 6.1.6 from the normal updater.
- About **39%** are Joomla 5 sites already running a 6.x build. These see no update and need the 6.1.6 package installed by hand.
- About **27%** are Joomla 3 sites on the 3.x line, with no fixed release.
- A few percent are on the 4.x and 5.x lines, offered 4.0.9 or 5.1.3, both still unprotected.

Add those up and roughly seven in ten affected installs cannot get the fix from Joomla's update screen. The largest single group is not the old Joomla 3 sites but the Joomla 5 sites that did the right thing, moved to the 6.x line early, and are now told nothing is available.

An empty update list is not proof you are patched

On Joomla 3, 4 and 5, Phoca Download can show no available update while running a vulnerable version, or offer an update that is itself unprotected. Check the installed version under System, Manage, Extensions and compare it with 6.1.6 by eye.

What to do about Phoca Download on each Joomla version

1. **Joomla 6:** update Phoca Download to 6.1.6 through the normal Joomla updater, then confirm the version number.
2. **Joomla 5 already on a 6.x build:** take a backup, then install the 6.1.6 package by hand from the [GitHub release](#). The updater will not offer it.
3. **Joomla 3, 4 or 5 on the 3.x, 4.x or 5.x line:** there is no fixed release for you. Remove front-end users and groups from each category's Delete Rights, which closes the path because the tasks reject users without that right. Then plan the move to Joomla 6, or remove the component if the site no longer needs it.
4. **On any Joomla version:** if Delete Rights were ever granted to front-end users, check the file list in each of those categories for files that are missing or unpublished and that no one meant to remove.

See which of your sites are still on Joomla 3, 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 Download installs

The Phoca Download version alone does not tell you what to do. You need the Joomla version next to it, because that decides whether the updater will deliver 6.1.6, whether

you need the package by hand, or whether the only options are the mitigation and a move to Joomla 6.

mySites.guru keeps both for each connected Joomla site. We added this flaw to our [vulnerability database](#) on 26 October 2026, so every site running Phoca Download below 6.1.6 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 5 sites for the manual package and the older lines for the Delete Rights check. That works the same way across a [portfolio of Joomla sites](#) of any size, and is part of every [subscription](#).

Why a Low score on Phoca Download still matters for older Joomla sites

Taken alone, this flaw is a footnote. Someone with Delete Rights has to be logged in and has to load the wrong page, and the worst outcome is a file gone from a category where that person could have deleted it anyway. Phoca fixed it, the fix is clean, and we would not write a post about a 2.3 Low if it stopped there.

The pattern matters more than the score. Several Phoca security fixes this year have left older Joomla lines without a fixed release. The [Phoca Download upload flaw](#) in July, which we found and reported and Phoca fixed the same day, was patched on the 6.x line only. The [Phoca Cart product filter SQL injection](#) in August reached the Joomla 5 and 6 lines and left Joomla 3 and 4 behind, the [Phoca Cart download IDOR](#) in October was fixed on 6.x alone, and the [Phoca Gallery EXIF stored XSS](#), published three days before this release, left Joomla 4 and 5 with versions that look current and are not. Phoca is quick with each fix. The release notes never say which lines were left out, and the updater on an older Joomla either offers a number that is still vulnerable or offers nothing.

If you look after Joomla 3, 4 or 5 sites that run any Phoca extension, treat every Phoca security release as one you have to check by hand. Read the manifest, compare the version the updater offers with the one that has the fix, and assume the gap is there until you have proved it is not. The next one may not be a Low.

Further Reading

- [Phoca Download 6.1.6 on GitHub](#) - the security release, with the package download for a manual install.
- [Phoca Download 6.1.6 release announcement](#) - Phoca's news post naming the fix as a cross-site request forgery.
- [Phoca Download update manifest](#) - the feed that decides which Phoca Download each Joomla version is offered.
- [CWE-352: Cross-Site Request Forgery](#) - the weakness class for a state-changing request that is not checked for the user's intent.
- [OWASP Cross-Site Request Forgery Prevention Cheat Sheet](#) - why a form token is the standard defence and why a GET request should never change state.

Frequently Asked Questions

What did Phoca Download 6.1.6 fix?

A cross-site request forgery flaw in the front-end User Control Panel's file actions. Before 6.1.6 the publish, unpublish and delete tasks checked only that the logged-in user held the category's delete right and never checked Joomla's anti-CSRF form token. In 6.1.6 all three go through one shared handler that checks the token first.

Is there a CVE for the Phoca Download 6.1.6 fix?

Not yet. Phoca's news post says more details will be available in the CVE record, but no record had been published as of 26 October 2026. The 2.3 Low score on this page is our own CVSS 4.0 assessment of the released code, not a vendor or CNA figure.

Is my site exposed to the Phoca Download CSRF flaw?

Only if a front-end user or group has been granted Delete Rights on a Phoca Download category. Delete Rights are closed by default, so a site where no front-end user holds them on any category is not exposed. There is no confidentiality impact and no code execution.

Which Phoca Download versions are affected?

Every release line below 6.1.6. We extracted 2.1.9, 3.2.3, 4.0.9, 5.1.3 and 6.0.0 and none of them checks the token on these tasks. Only the Joomla 6 line, at 6.1.6, has the fix; the Joomla 3, 4 and 5 lines have no fixed release.

Why does my Joomla 5 site not offer the Phoca Download 6.1.6 update?

Phoca's update manifest offers Joomla 5 sites version 5.1.3. If your site already runs a 6.x build, Joomla's updater discards the lower version and shows no update at all. Take a backup and install the 6.1.6 package by hand from the GitHub release.

Can mySites.guru show me which sites run a vulnerable Phoca Download?

Yes. The flaw was added to the mySites.guru vulnerability database on 26 October 2026, so every connected Joomla site running Phoca Download below 6.1.6 is flagged on its dashboard, with the Joomla version on the same screen so you can see which sites the updater will serve and which need the package by hand.

AI MODIFIED

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

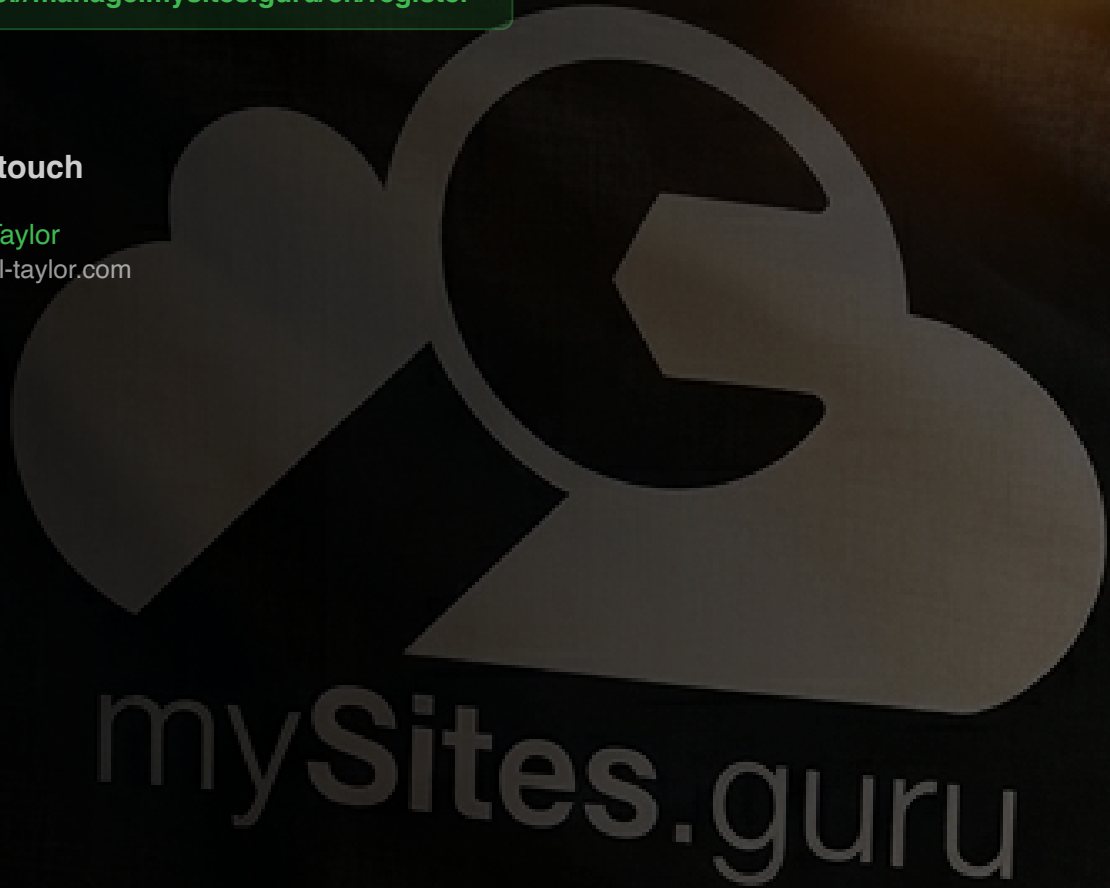
Get Your Free Site Audit

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

