



Phoca Cart 6.1.9 stops anyone downloading other customers' paid files

Phoca Cart before 6.1.9 let anonymous visitors download the digital products other customers bought. Only the Joomla 6 line is fixed, and 6.1.8 is affected.

Phil E. Taylor | 1 October 2026

On 1 October 2026 Phoca released Phoca Cart 6.1.9, a security release for the Joomla e-commerce extension. The announcement names the flaw in one line: "Authorisation bypass through user-controlled key (IDOR) in Order View", with more detail promised in a CVE record that has not appeared yet.

We read the 6.1.9 package to work out what that means for a shop. It means anyone could download the digital products your other customers paid for, without an account. If your shop sells downloads, anyone could have taken your stock for free.

TL;DR

- Phoca Cart before **6.1.9** checked that a download token and an order token had been sent with a download request, but **never checked that they were correct**
- Any visitor, **logged in or not**, could fetch any purchased file by its sequential id, and each fetch counted against the real buyer's download limit
- **6.1.8 is affected**. Shops that installed the August security release need to update again
- **Only the Joomla 6 line is fixed**. The current releases for Joomla 5 (5.2.4), Joomla 4 (4.0.13) and Joomla 3 (3.5.8) contain the same code and no fix
- Joomla 5 sites will not be offered 6.1.9 by the updater. Install the package by hand
- No CVE has been published yet. This is Phoca's fix; we analysed the release after it shipped

8.7

CVSS 4.0

Unauthenticated download of other customers' purchased files

HIGH

mySites.guru assessment, pending the CVE record

Any visitor can download every digital product sold through the shop, along with whatever else was attached to an order as a download. Nothing on the site is changed.

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

No login needed

Paid files exposed

No fix on Joomla 3, 4 or 5 lines

▼ 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:N None: Nothing can be altered

VA:N None: The site stays up

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 Cart download check failed

When a customer buys a downloadable product, Phoca Cart creates a row for the file against their order and gives it a download token. The order has its own token too. A guest buyer downloads the file by sending both tokens back, and a logged-in buyer is recognised as the owner of the order.

The download task in `admin/libraries/phocacart/download/download.php` loaded the file row from the numeric id in the request, then ran its ownership check. Here it is from 6.1.8:

```
// CHECK USER AND TOKEN
if ((int)$user->id < 1 && ($tokenDownload == '' || $tokenOrder == '')) {
    return false;
}
if (!isset($file->userid) && ($tokenDownload == '' || $tokenOrder == ''))
    return false;
}
if ($user->id != $file->userid && ($tokenDownload == '' || $tokenOrder == ''))
    return false;
}
```

Each condition ends in “the token is empty”. None of them compares the token sent with the token stored. So a visitor who is not the owner gets through by sending any two non-empty strings as **d** and **o**. The file ids are sequential integers, so finding the files takes nothing more than counting.

The only other gate in front of it is Joomla’s form token check in the download controller. That is a protection against cross-site request forgery, not a login, and any visitor receives one from a page with a form.

The download limits in Phoca Cart’s settings still applied, and that has a side effect a shop owner should know about. Each stolen download added to the file’s hit count, so a buyer whose shop limits the number of downloads may have found their allowance used up by someone else.

What changed in Phoca Cart 6.1.9

The fix is thirteen lines in the same function. The visitor now has to be the logged-in owner of the order, or send both tokens and have each match the stored value, compared with `hash_equals()` :

```
$isOwner = ((int)$user->id > 0 && isset($file->userid) && (int)$user->id == $file->userid) ? true : false;

if (!$isOwner) {
```

```

        if ($tokenDownload === '' || $tokenOrder === ''
            || !isset($file->download_token) || !isset($file->order_token)
            || !hash_equals((string)$file->download_token, (string)$tokenDownload)
            || !hash_equals((string)$file->order_token, (string)$tokenOrder))
            return false;
    }
}

```

That is the check the old code meant to perform. The only other code change in the release is a loose comparison in the order status handler, which is not security related. If you diff the GitHub tags rather than the packages, you will also see output escaping in the filter layouts. That belongs to 6.1.8: its tag was cut 43 seconds before the commit with the escaping, so the tag compare shows it under 6.1.9. We confirmed both points against the released ZIPs rather than the tags.

What we did and did not test

This is a reading of the released code, not an attack on anyone's shop. We have not requested a file from any live site, and we are not publishing a working request.

Which Phoca Cart versions are affected?

All versions before 6.1.9, on all four branches. Phoca maintains one release line per Joomla version, and only the Joomla 6 line received the fix:

Joomla version	Newest Phoca Cart offered by the updater	Has the download fix?
Joomla 6	6.1.9	Yes
Joomla 5	5.2.4	No
Joomla 4	4.0.13	No
Joomla 3	3.5.8	No

We checked the download function in each of those packages. 5.2.4 and 4.0.13 are identical to 6.1.8, and 3.5.8 has the same empty-token checks. That table comes from Phoca's update manifest as it stood on release day.

Look twice at the 6.1.8 row, because 6.1.8 was itself a security release. It fixed the price filter cross-site scripting issues (CVE-2026-76564 and CVE-2026-76565) in August, a few days after 6.1.7 fixed the product filter SQL injection. A shop that did everything right this summer is on 6.1.8 today, and it is exposed. Among the Phoca Cart installs we can see, roughly two in three of the affected ones are on 6.1.8.

Joomla 5 shops have to install Phoca Cart 6.1.9 by hand

This is the same distribution problem we described with the SQL injection in August. Phoca's update feed offers each Joomla version one release, matched on a `targetplatform` regex, and Joomla discards any offered version that is not higher than the one installed.

On Joomla 5 that produces two different failures:

- **A Joomla 5 site on Phoca Cart 6.x** is offered 5.2.4, which is lower than what it has. Joomla shows no update at all, and the site looks current while it runs 6.1.8.
- **A Joomla 5 site on Phoca Cart 5.x** below 5.2.4 is offered 5.2.4. That release fixed the August SQL injection and does nothing for this flaw, so a site owner can apply the update in good faith and still be exposed.

Phoca Cart 6.x installs and runs on Joomla 5, so the fix for both is the same: download `pkg_phocacart_v6.1.9.zip` from the 6.1.9 release and install it through Joomla's extension installer. Take a backup first, as with any jump across a major version.

Across the Joomla sites we manage, about half of the vulnerable Phoca Cart installs are on Joomla 3, 4 or 5, where the updater will not deliver this fix. Roughly one in ten is on Joomla 3 or 4, where no fixed release exists at all.

An empty update list is not proof you are patched

On Joomla 5, Phoca Cart can show no available update while running a vulnerable version. Check the installed version under System, Manage, Extensions and compare it with 6.1.9 by eye.

What to do about it on each Joomla version

1. **Joomla 6:** update Phoca Cart to 6.1.9 through the normal Joomla updater, then confirm the version number.
2. **Joomla 5:** install `pkg_phocacart_v6.1.9.zip` by hand from the [GitHub release](#). Do not take the 5.2.4 the updater offers as a fix for this.
3. **Joomla 3 and Joomla 4:** there is no fixed Phoca Cart for your Joomla version, which fits a pattern we covered in the [J2Store 3 end-of-life post](#): Joomla 3 shop extensions stop getting fixes long before their product pages say so. The lasting fix is to move the site to Joomla 5 or 6 and then to Phoca Cart 6.1.9. Until then, if the shop sells downloads, block requests whose `task` is `download.download` at your firewall or web server. That stops paying customers downloading too, so send purchased files to buyers another way while it is in place.
4. **On any Joomla version:** if the shop sells downloadable products, assume the files may have been copied. Look in your web server logs for download task requests in volume or from addresses that never bought anything, and expect buyers to report download limits already reached.

A shop that sells only physical goods has no order downloads for this flaw to hand out. Update anyway: the code is installed, and a downloadable product added next year would be exposed from the moment it went on sale.

See which of your sites are still on Joomla 3 or 4

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 Cart installs

The awkward part of this release is that the Phoca Cart version alone does not tell you what to do. You need the Joomla version beside it, because that decides whether the updater will help, whether you need the package by hand, or whether there is no fix at all.

mySites.guru keeps both for each connected Joomla site. We added this flaw to our [vulnerability database](#) on release day, so every site running Phoca Cart below 6.1.9 is flagged on its dashboard now, with the Joomla version on the same screen. The Joomla 6 sites can then go out in one batch with the [mass updater](#), which leaves a short list of Joomla 5 shops 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 download checks keep failing in shop extensions

An IDOR happens when code checks the wrong thing. The code here knew it had to decide whether this visitor was allowed this file, and it had the right ingredients on hand: the stored tokens were loaded in the same query as the file. It tested whether the visitor had sent something, rather than whether what they sent was right.

It is the same shape as the [Events Booking invoice flaw](#) we covered in July, where anyone could download any registrant's invoice by its id. Paid downloads are where this hurts most, because the file is the product. A leaked order number exposes an address; a leaked download hands over the thing the shop exists to sell, at no cost, as many times as the limits allow. When you review any Joomla shop extension, follow the

download path first and look for the comparison against stored data. It is the line that most often turns out to be missing.

Phoca has been quick with fixes this year, with three security releases of Phoca Cart since August. The gap is on the older lines. Of those three, only the August SQL injection fix reached every branch from Joomla 4 up, and this one reached Joomla 6 only. A shop on an older Joomla version gets fewer fixes from each release, and the announcements do not say which lines were left out.

Further Reading

- [Phoca Cart 6.1.9 security release announcement](#) - Phoca's own notice, which names the flaw as an IDOR.
- [Phoca Cart 6.1.9 on GitHub](#) - the release with both the component and full package downloads.
- [Phoca Cart update manifest](#) - the feed that decides which Phoca Cart each Joomla version is offered.
- [CWE-639: Authorization Bypass Through User-Controlled Key](#) - the weakness class Phoca named.
- [OWASP: Insecure Direct Object Reference Prevention](#) - why a record id in a request is never proof of ownership.

Frequently Asked Questions

What did Phoca Cart 6.1.9 fix?

An authorisation bypass in the download of purchased files. Before 6.1.9 the download task only checked that a download token and an order token had been sent, never that they were the right ones, so any visitor could fetch another customer's paid digital product by its numeric id.

Do I need to be logged in to exploit the Phoca Cart download flaw?

No. A logged-out visitor who sends any non-empty value for both tokens passes the check. The only other thing the request needs is Joomla's form token, which any visitor gets from a page with a form on it.

Which Phoca Cart versions are affected?

Every version before 6.1.9. That includes 6.1.8, the release that fixed the price filter XSS in August, and the current releases on the older lines: 5.2.4, 4.0.13 and 3.5.8 all contain the same unchecked code and have no fixed release.

Does this affect a Phoca Cart shop that only sells physical goods?

Not in practice. The flaw exposes files attached to orders as downloads, so a shop with no downloadable products has nothing for it to hand out. The vulnerable code is still installed, so update anyway.

Why does Joomla 5 not offer the Phoca Cart 6.1.9 update?

Phoca's update feed offers 5.2.4 to Joomla 5 sites and 6.1.9 only to Joomla 6 sites. A Joomla 5 site running 6.x sees a lower version and reports no update, and one running 5.x is offered 5.2.4, which does not contain this fix. Phoca Cart 6.x runs on Joomla 5, so install the 6.1.9 package by hand.

Is there a CVE for the Phoca Cart 6.1.9 fix?

Not yet. Phoca's announcement says the details will appear in the CVE record, which had not been published when this post went out. We will add the id here when it is.

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

Yes. mySites.guru flags every connected Joomla site running Phoca Cart below 6.1.9 on its dashboard, and shows the Joomla version beside it, which you need here to know whether

the updater will offer the fix.

AI MODIFIED

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

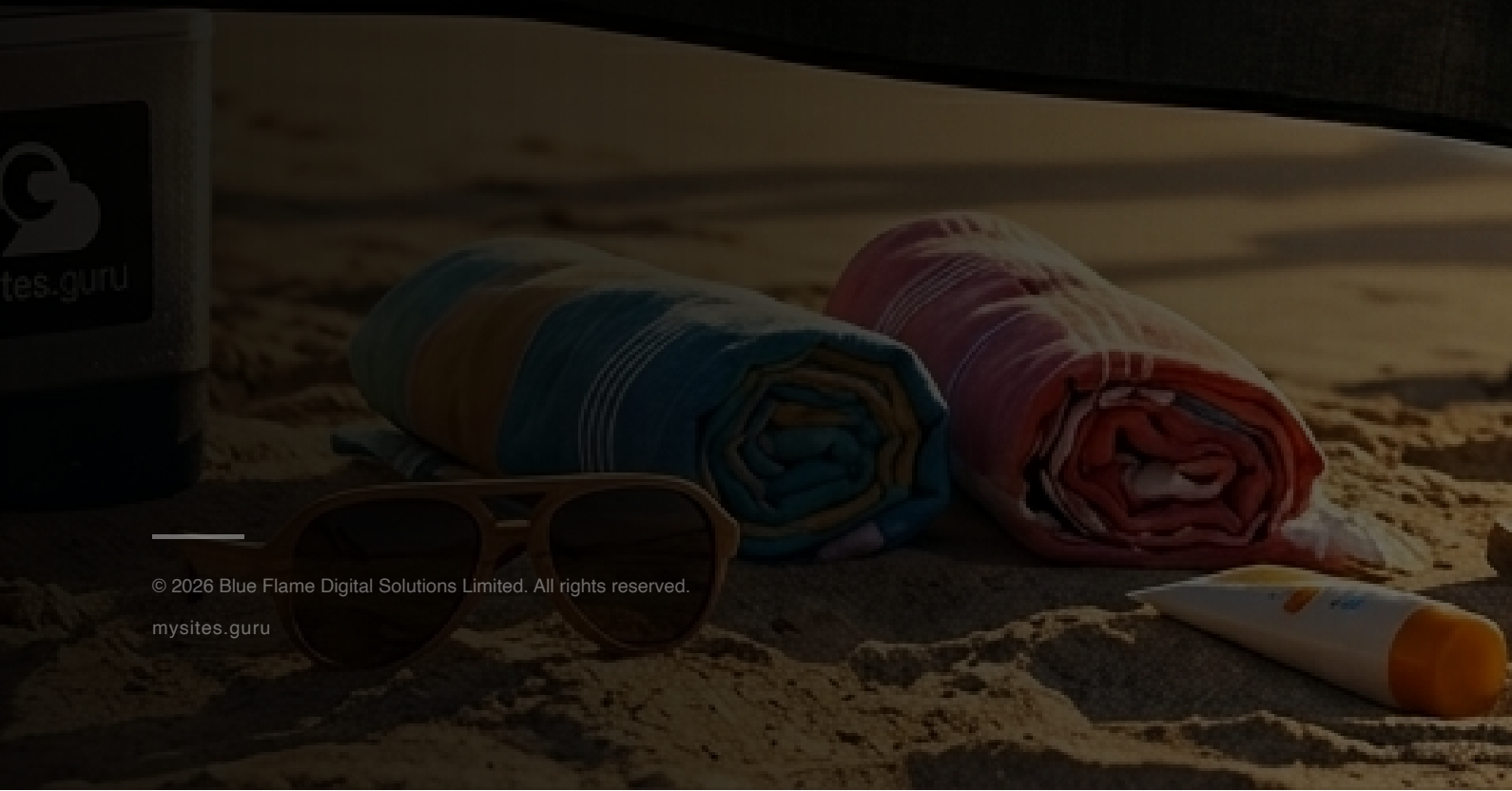
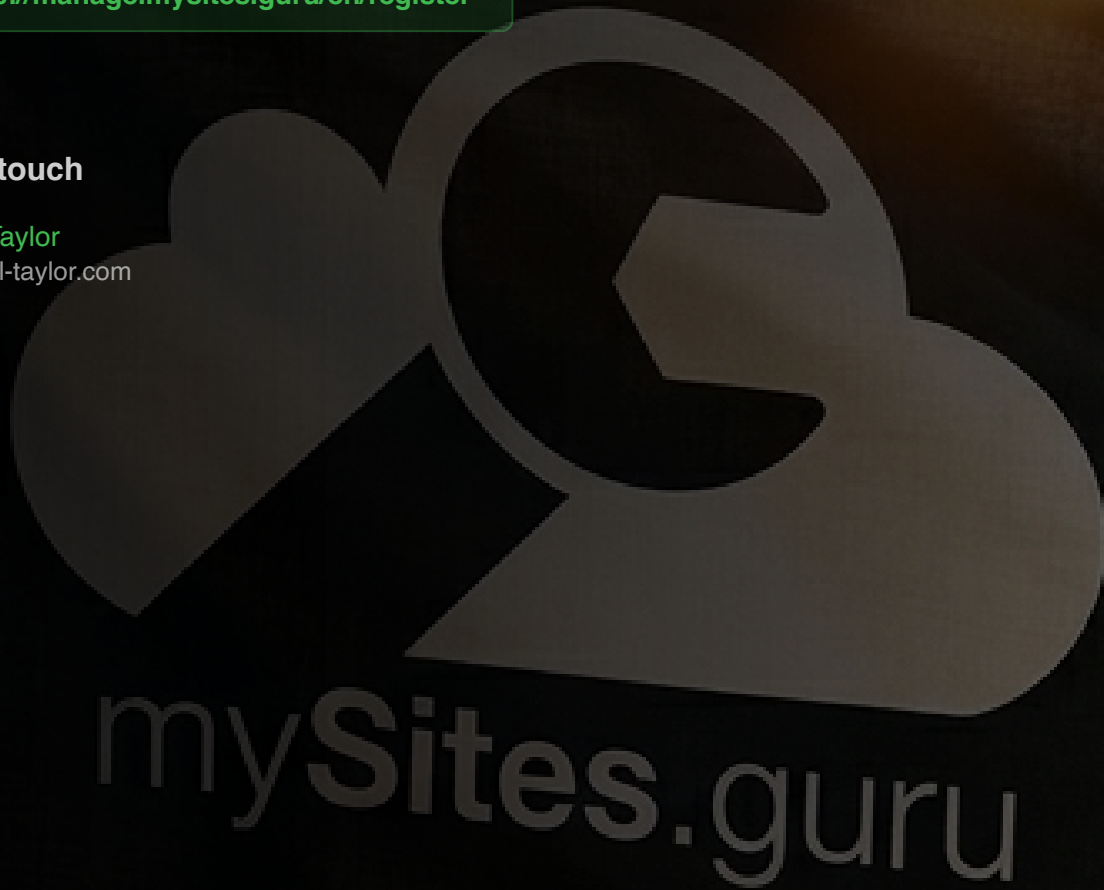
Get Your Free Site Audit

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