mySites.guru

HikaShop 6.8.1 Stops Visitors Downloading Paid Product Files

HikaShop 6.8.1 closes a route that let any visitor download files from the secure upload folder, paid product files included. Who is affected and what to do.

Phil E. Taylor | 5 November 2026

TL;DR

HIKARI SOFTWARE released HikaShop 6.8.1 on Thursday 5 November 2026, a few hours after HikaShop 6.8.0 went out the same day. Before 6.8.1, a visitor to a HikaShop site could type the name of a file into an ordinary text custom field, an engraving line on a cart item or the name on an address, and then fetch that file through HikaShop's own download feature. The file came from the secure upload folder, which is where HikaShop keeps the files of the downloadable products customers pay for. No login was needed. 6.8.0 is not enough: the check that closes the route is in 6.8.1.

HikaShop is a Joomla e-commerce extension by HIKARI SOFTWARE, sold in three editions: Starter (free), Essential and Business. This is a flaw in the Joomla extension, not in Joomla itself, and all three editions have it below 6.8.1. No CVE has been published, the vendor credits no researcher, and the vendor says nothing about exploitation.

8.2
CVSS 4.0

HikaShop below 6.8.1: secure upload folder files downloadable through a text custom field

HIGH **mySites.guru assessment**

Any visitor who knows the name of a file in HikaShop's secure upload folder can download it without logging in or buying anything, paid product files included.

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

No login needed | Exploitable over the internet | Needs the file name | Paid files exposed

▼ 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: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

What Changed in HikaShop 6.8.1

The 6.8.1 changelog has one entry under Security, and it describes the flaw in full: “A download link naming a custom field that is not an upload field (a text field such as a cart item’s engraving or an address name) is now refused on the frontend; before, a visitor who typed the name of a file of the secure upload folder in such a field could then download that file, purchased product files included.”

The packages match that description. The 6.8.0 changelog, released earlier on the same day, has a single security line with no detail at all: “A security issue related to downloadable files is fixed.” Whatever 6.8.0 changed, the check that stops a text field being used to pull a file from the secure upload folder is the one in 6.8.1, so 6.8.0 on its own is not the fixed version.

How the HikaShop Download Check Worked, and What 6.8.1 Adds

HikaShop lets a shopper upload a file through a custom field, an image to be printed on a mug, say, attached to a cart item, and later download it again. That download goes through the file class’s custom-field download function, which checks that the visitor is allowed the file before serving it.

On the frontend, the check confirmed one thing: that the requested file name matched the value saved in the named custom field, for the visitor's own cart, checkout session, order, user record or address. What it did not confirm was that the field was an upload field at all. A text field is a custom field too, and HikaShop ships with plenty of them: address fields are text fields, and so is the engraving line a shop might add to a cart item.

So the route was short. A visitor types a file name into a text custom field, HikaShop saves it as the field's value, and the visitor then asks the download feature for that field. The saved value matches the request, the check passes, and HikaShop serves the file with that name from the secure upload folder. The default location of that folder is media/com_hikashop/upload/safe/, and it holds two kinds of file: the ones shoppers upload through custom fields, and the files of downloadable products that customers pay for.

6.8.1 adds one check. On the frontend, the field named in the request must be a file or image upload field (HikaShop's file, image, ajaxfile and ajaximage field types), and any other field type is turned away before a file is looked up. The change is in the file class, in the custom-field download function, and it is the same change in every edition.

Three limits set the severity:

- The download feature already blocked ".." in the file name, so only files inside the secure upload folder and its subfolders were reachable. The rest of the server was not.
- The visitor has to know, or guess, the exact file name. There is no listing.
- No login is needed. A guest's cart and checkout fields count, and text custom fields are standard in HikaShop, so the precondition in practice is the file name alone.

The mySites.guru CVSS 4.0 vector is CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N: reachable over the network, low complexity, no privileges, no user interaction, high confidentiality impact and nothing on integrity or availability. The AT:P metric, attack requirements

present, records that the attacker needs something they do not get from the flaw itself, the file name. The score is 8.2 High.

A file name is not a secret in the way a password is, though. A product file named after the product, or a shop whose downloads follow a pattern, puts the name within reach of someone who has bought one file and wants the rest. The CVSS score is about the general case, and the general case for a shop selling ebooks, software, music, courses or sheet music is that the files it charges for could be taken without a purchase. The personalisation images shoppers upload sit in the same kind of folder.

Which HikaShop Sites and Joomla Versions Are Affected?

Every HikaShop site below 6.8.1, in every edition. The same code and the same fix are in the free Starter 6.8.1 package and in Business 6.8.1, so Starter, Essential and Business are all affected below 6.8.1 and all fixed in 6.8.1.

There is also one release line rather than several. The 6.8.1 update feed offers the same version to Joomla 3 sites as to Joomla 4, 5 and 6, so a Joomla 3 shop is not left waiting on a separate branch. A Joomla 3 shop can take this fix today, and HikaShop's Joomla 3 support has its own entry on joomla3security.com.

HikaShop version	Status	What to do
6.8.1	Fixed	Nothing further
6.8.0	Affected	Update to 6.8.1
Below 6.8.0	Affected	Update to 6.8.1

On the evening of release day, this is what the HikaShop sites in the mySites.guru database looked like:

96%

11%

of HikaShop sites
below 6.8.1, in every edition

of HikaShop sites
on 6.8.0, which is not enough

3%
of HikaShop sites
already on 6.8.1

HikaShop sites in the mySites.guru database on the evening of 5 November 2026.

The single most common version was 6.7.1, at about three sites in ten. The 11% on 6.8.0 is the figure to watch. Those shops updated on the day, and because 6.8.0 reached them first, the update notice cleared for a few hours and then came back when 6.8.1 followed. A site that only looks at the update notice once will think it is done.

What To Do on a HikaShop Site Now

1. Update HikaShop to 6.8.1 through the Joomla updater. 6.8.0 is not enough. There is no setting in older versions that switches this off, so the update is the fix.
2. If you sell downloadable products, look in the web server access logs for frontend requests to HikaShop's order download feature that name a custom field, from visitors who had not bought the file. The access log is where those requests show up.
3. If you have many HikaShop sites, update them all in one pass rather than one at a time. The 6.8.0 and 6.8.1 pair shows why: a shop updated by hand to 6.8.0 was on an affected version again as soon as 6.8.1 followed.

Two updates on one day, and only the second one counts

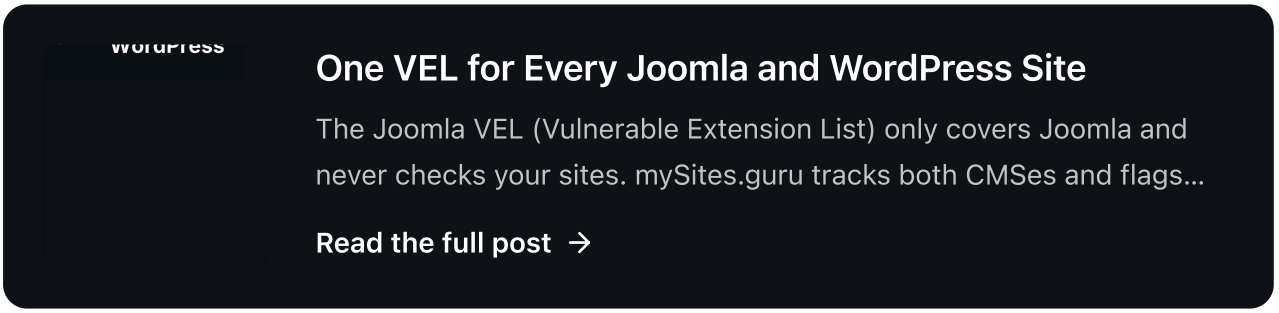
HikaShop 6.8.0 and 6.8.1 both went out on 5 November 2026 and both mention downloadable files. A site that took the first update and stopped is still affected. Check the installed version, not the date you last updated.

Extension updates that arrive in pairs like this are a good argument for letting Joomla apply extension updates on its own. The guide to enabling Joomla extension auto-updates covers how, and which extensions it is sensible for.

How mySites.guru Flags HikaShop

On 5 November 2026 we added a rule that flags every connected Joomla site running the HikaShop component below 6.8.1, in every edition. Flagged sites appear in the vulnerable extension list with their installed version, so a 6.8.0 site stands out from a 6.8.1 one. An earlier rule already flags HikaShop below 6.5.2 for an older open redirect flaw, rated Low, and the HikaShop page lists both.

The mass updater then does the rest: bulk updating Joomla extensions across many sites at once, so the 6.8.0 sites and the 6.7.1 sites reach 6.8.1 in the same run. Every rule we hold is on the public vulnerabilities page, and the flags and the updater are part of the subscription.



If a site has already been hit, or you would rather someone else made sure, fix.mySites.guru patches the site, audits it for backdoors and hands it back secure for a single fixed fee, usually the same day.

Timeline

2026-11-05 ● **HikaShop 6.8.0 released**

The changelog's only security line: "A security issue related to downloadable files is fixed."

2026-11-05

HikaShop 6.8.1 released

Frontend downloads through a custom field that is not an upload field are turned away, closing the route to files in the secure upload folder.

2026-11-05

mySites.guru flags affected sites

A rule flags every connected Joomla site on HikaShop below 6.8.1, in every edition.

Further Reading

- HikaShop 6.8.1 changelog - the release notes with the Security entry describing the custom field download fix.
- HikaShop 6.8.0 changelog - the earlier release the same day, with its one-line security entry.
- HikaShop on joomla3security.com - HikaShop's Joomla 3 support and what that means for shops still on Joomla 3.
- J2Store 3 End of Life - another Joomla e-commerce extension, and what running an unsupported shop looks like.

Frequently Asked Questions

Which HikaShop version fixes the paid file download flaw?

HikaShop 6.8.1, released by HIKARI SOFTWARE on 5 November 2026. It adds a check on the frontend that a custom field named in a download request must be a file or image upload field. Every release below 6.8.1 should be treated as affected, in every edition.

Is HikaShop 6.8.0 enough?

No. HikaShop 6.8.0 went out earlier on the same day with the line "A security issue related to downloadable files is fixed" and no more detail. The check that stops a text custom field being used to fetch a file from the secure upload folder is in 6.8.1, so a site on 6.8.0 still needs the update.

Is there a CVE for the HikaShop 6.8.1 security fix?

No CVE has been published at the time of writing. HIKARI SOFTWARE credits no researcher, says nothing about whether the flaw was exploited, and the flaw is not in CISA's Known Exploited Vulnerabilities list. mySites.guru's own CVSS 4.0 assessment is 8.2 High.

Does an attacker need to be logged in to a HikaShop site?

No. A guest's cart and checkout fields count, so no account is needed. What the attacker does need is the exact file name inside HikaShop's secure upload folder, either known or guessed. That requirement is the attack requirement (AT:P) in the 8.2 High score.

Does the flaw affect the free HikaShop Starter edition?

Yes. The same code and the same fix are in the free Starter 6.8.1 package and in Business 6.8.1, so Starter, Essential and Business are all affected below 6.8.1 and all fixed in 6.8.1. The update feed offers 6.8.1 to Joomla 3 sites as well as Joomla 4, 5 and 6.



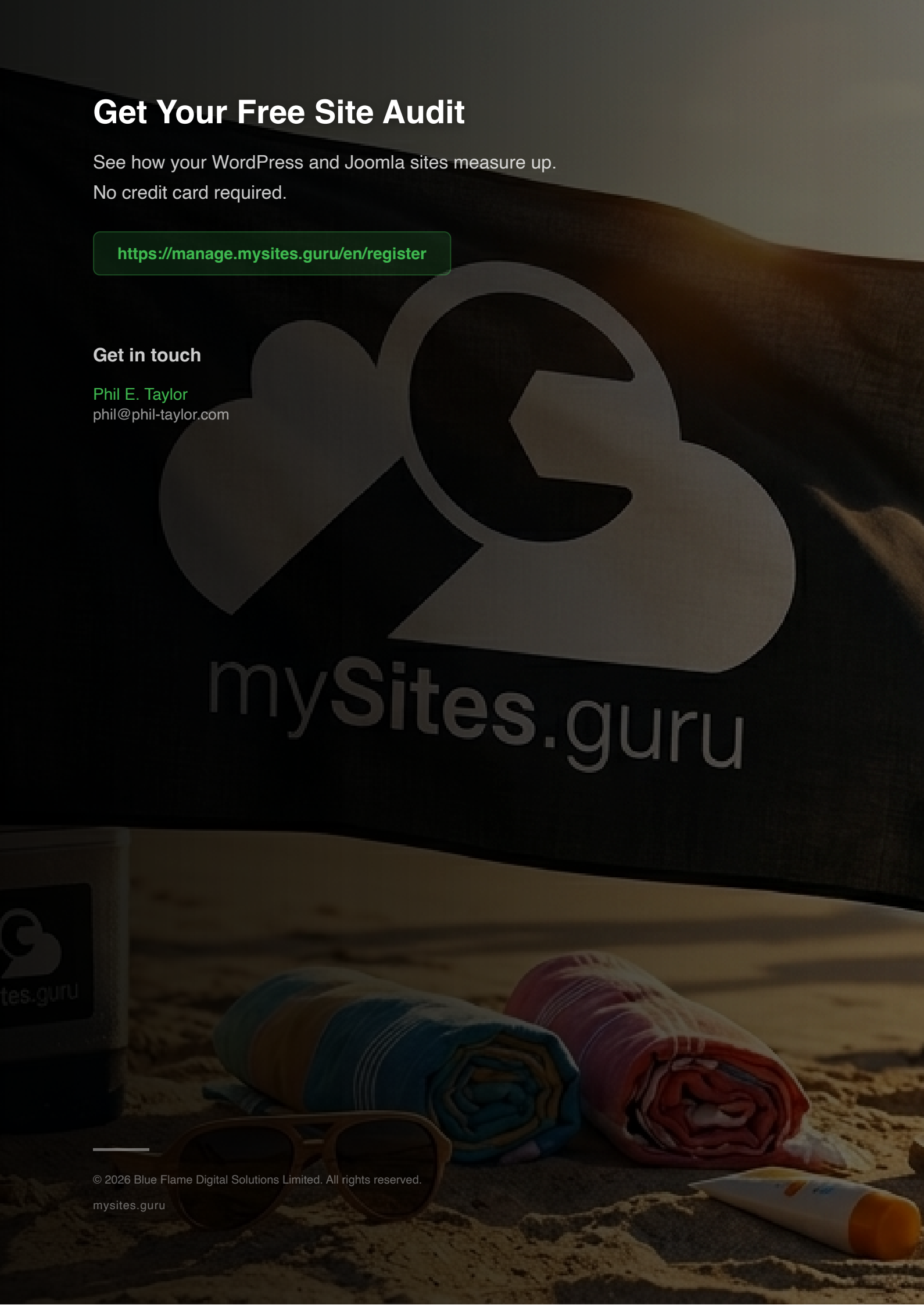
Written and edited by a human, with AI assistance. Our approach to AI

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.