



YOOtheme Pro 5.0.53 Fixes an Unauthenticated RCE: Update Every Site Now

YOOtheme Pro 5.0.53 fixes CVE-2026-102785, an unauthenticated remote code execution flaw in the image handler. Update every Pro 5 site now; Pro 4 is unaffected.

Phil E. Taylor | 21 October 2026

YOOtheme has released YOOtheme Pro 5.0.53, the critical security update for its Joomla page-builder template that it gave advance notice of the day before. The changelog entry names the flaw: CVE-2026-102785, "Fix unauthenticated remote code execution via image handler". Every YOOtheme Pro 5 build from 5.0.0 to 5.0.52 is affected. Update every site running one of them to 5.0.53 or later now. YOOtheme Pro 4 and earlier are not affected.

This was the vendor's notice to customers on 20 October 2026: "We are preparing a critical security update for YOOtheme Pro 5, scheduled for release October 21, at 4 PM CEST. All users running YOOtheme Pro 5 must update immediately once the new version becomes available. YOOtheme Pro 4 and earlier versions are not affected." The release came out ahead of that slot, and by early afternoon UTC sites were already updating.

9.3

CVSS 4.0

CVE-2026-102785: unauthenticated remote code execution via the image handler

CRITICAL

mySites.guru (provisional, the CVE record is not published yet)

Any visitor could reach the public image handler without logging in and, in 5.0.52 and earlier, influence what the handler wrote to disk and where, which the vendor classifies as remote code execution.

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

I:N/SA:N

No login needed

YOOtheme Pro 5.0.0 to 5.0.52

Fixed in 5.0.53

▼ 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:H High: Data and files can be altered at will
VA:H High: The site can be taken down

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

The score above is our own assessment, taken from the vendor's classification of the flaw as unauthenticated remote code execution. The CVE identifier is reserved but its record has not been published yet, so there is no official CVSS score, CWE or description to quote. We will update the [YOOtheme entry in the Joomla Vulnerability Database](#) when the record appears. Who reported the flaw to YOOtheme has not been stated.

What the YOOtheme Pro 5 Joomla template flaw is

The flaw is in the image handler, the public route YOOtheme Pro uses to generate and cache resized and cropped images. The image URLs YOOtheme Pro generates on a site's pages point at it, and any visitor can reach it without logging in. That is what makes this different from the two earlier YOOtheme Pro 5 security releases this year, 5.0.41 and 5.0.42 in August, which each fixed flaws that needed a privileged account.

Comparing the 5.0.52 and 5.0.53 packages shows what changed. In 5.0.52 the handler let the request choose which image operations to run, and it did not tie the cache file name it writes to the signed image URL. In 5.0.53 the operations are limited to a fixed list (type, crop, resize, rotate, flip and thumbnail), and the handler checks that the cache file name matches the signed URL before writing anything. Put the two together and in 5.0.52 a request could influence both what was written and where, with no account on the site. YOOtheme calls that remote code execution, and we have no reason to disagree.

That is as far as we will go. The record is not published, the patch is hours old, and a worked example would help the wrong people more than it would help you.

A malicious actor's own code runs on your server, with the same access as the website itself: reading, changing or deleting any file it can touch, planting a backdoor that survives the next update, installing malware, pulling every database credential and API key from your configuration, and using your server to attack other people. Gulp.

The image handler is a public endpoint on any site running YOOtheme Pro 5, so an unpatched site is exposed to anyone who can load a page on it. Treat every site still on 5.0.52 or earlier as exposed until it is on 5.0.53, and check it for signs of tampering once it is.

Why YOOtheme Pro 4 Joomla sites are not affected

YOOtheme's notice says YOOtheme Pro 4 and earlier are not affected. So the first job is a version check: a site still on YOOtheme Pro 4 has nothing to do for this issue, and a site on any 5.0.x build from 5.0.0 to 5.0.52 needs the update.

YOOtheme publishes one changelog for both its Joomla and WordPress editions, and 5.0.53 is the release for both, so a WordPress site running YOOtheme Pro 5 needs the same update.

mySites.guru flags affected YOOtheme Pro 5 Joomla sites

If you connect your Joomla sites to mySites.guru, the version check is done for you. A detection rule flags every connected Joomla site running YOOtheme Pro 5.0.0 to

5.0.52, so a site snapshot raises an alert telling you to update. The rule matches both the YOOtheme template and its system plugin, because YOOtheme Pro installs as both and updating YOOtheme Pro updates both. YOOtheme Pro appears in the [Joomla Vulnerability Database](#) alongside the other extensions we track, and the alert clears once a later snapshot sees 5.0.53 or later.

If you manage more than a handful of Joomla sites, the value is the list: one place that says which sites are still on an affected build. See [managing multiple Joomla sites](#) for how the rest of the workflow fits together, and a [free site audit](#) shows the same finding on a site you have not connected yet.

What Joomla site owners running YOOtheme Pro 5 should do now

Update to 5.0.53 or later, on every affected site, now. There is no partial mitigation, so the update is the fix.

1. Confirm which sites run YOOtheme Pro 5. Any build from 5.0.0 to 5.0.52 is affected; Pro 4 and earlier need no action.
2. Take a fresh [backup](#) of every affected site before updating. A backup is also your record of what the site looked like before any tampering.
3. Update every YOOtheme Pro 5 site to 5.0.53 or later immediately. The flaw needs no login, so every unpatched site is equally exposed. Update them in one window rather than the important ones first and the rest next week.
4. Check each site for signs of tampering after updating. The flaw was exploitable before the patch, so look for files that should not be there, such as unexpected PHP files in images, cache or media folders, and for anything changed recently. Run a mySites.guru audit on each site and read what it finds.
5. Re-snapshot each site in mySites.guru afterwards so the alert clears and the record shows the site on 5.0.53 or later.

Joomla page builders are a high-value target when no login is needed

A template framework like YOOtheme Pro sits on every page of a site and handles uploads, images and layouts for logged-in editors. When any of that handling can be reached without a login, it becomes a public endpoint on each site that runs the extension, and attackers treat it exactly that way. The same lesson came from [ZOO's unauthenticated file upload](#), another YOOtheme extension, and from the long run of extension disclosures collected in [a month of Joomla security disclosures](#).

So an available update to a template or page builder belongs on the security list, and [why an extension update is a security flag](#) makes that case in full. The window between a fix going public and the flaw being widely understood is short, so if you have been meaning to set up [automatic updates for Joomla extensions](#), this release is a good test of whether the process you have is fast enough.

Timeline

2026-10-20



YOOtheme gives advance notice of a critical YOOtheme Pro 5 security update

The vendor tells customers a critical fix is due the next day and that YOOtheme Pro 4 and earlier are not affected. mySites.guru adds a detection rule for YOOtheme Pro 5 the same day.

2026-10-21



YOOtheme releases 5.0.53 and names CVE-2026-102785 in the changelog

The changelog entry reads: Fix unauthenticated remote code execution via image handler. Update every YOOtheme Pro 5 site to 5.0.53 or later immediately.

Further Reading

- [YOOtheme Pro changelog](#) - the 5.0.53 entry naming CVE-2026-102785
- [YOOtheme Pro in the mySites.guru Joomla Vulnerability Database](#) - the entry that flags sites running 5.0.0 to 5.0.52
- [Treat an available Joomla extension update as a security flag](#) - why an extension update you have not applied is a security finding, not a chore

Frequently Asked Questions

Is my site affected by the YOOtheme Pro 5 vulnerability?

If it runs any YOOtheme Pro 5 build from 5.0.0 to 5.0.52, yes, until you update. YOOtheme Pro 4 and earlier are not affected, according to the vendor's notice.

Which version of YOOtheme Pro 5 fixes it?

YOOtheme Pro 5.0.53, released on 21 October 2026. Update every Pro 5 site to 5.0.53 or later.

Is there a CVE for the YOOtheme Pro 5 vulnerability?

Yes, CVE-2026-102785, which YOOtheme names in the 5.0.53 changelog entry. The identifier is reserved and the CVE record has not been published yet, so there is no official CVSS score or description at the time of writing.

Is the YOOtheme Pro 5 flaw remote code execution?

Yes. YOOtheme classifies it as unauthenticated remote code execution via the image handler, meaning an attacker needs no account on the site to exploit it. Our provisional score, pending the official record, is 9.3 Critical on CVSS 4.0.

Does the YOOtheme Pro 5 update apply to WordPress sites too?

Yes. YOOtheme publishes one changelog for its Joomla and WordPress editions and 5.0.53 is the release for both, so a WordPress site running YOOtheme Pro 5 needs the same update.

What should I do right now?

Take a backup, update every YOOtheme Pro 5 site to 5.0.53 or later, then check each site for files that should not be there and for recent unexpected changes, and run a fresh audit. There is no partial mitigation; the update is the fix.

Does mySites.guru detect the YOOtheme Pro 5 vulnerability?

Yes. A detection rule flags every connected Joomla site running YOOtheme Pro 5.0.0 to 5.0.52, matching both the template and its system plugin, and the alert clears once a later snapshot sees 5.0.53 or later.

AI MODIFIED

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

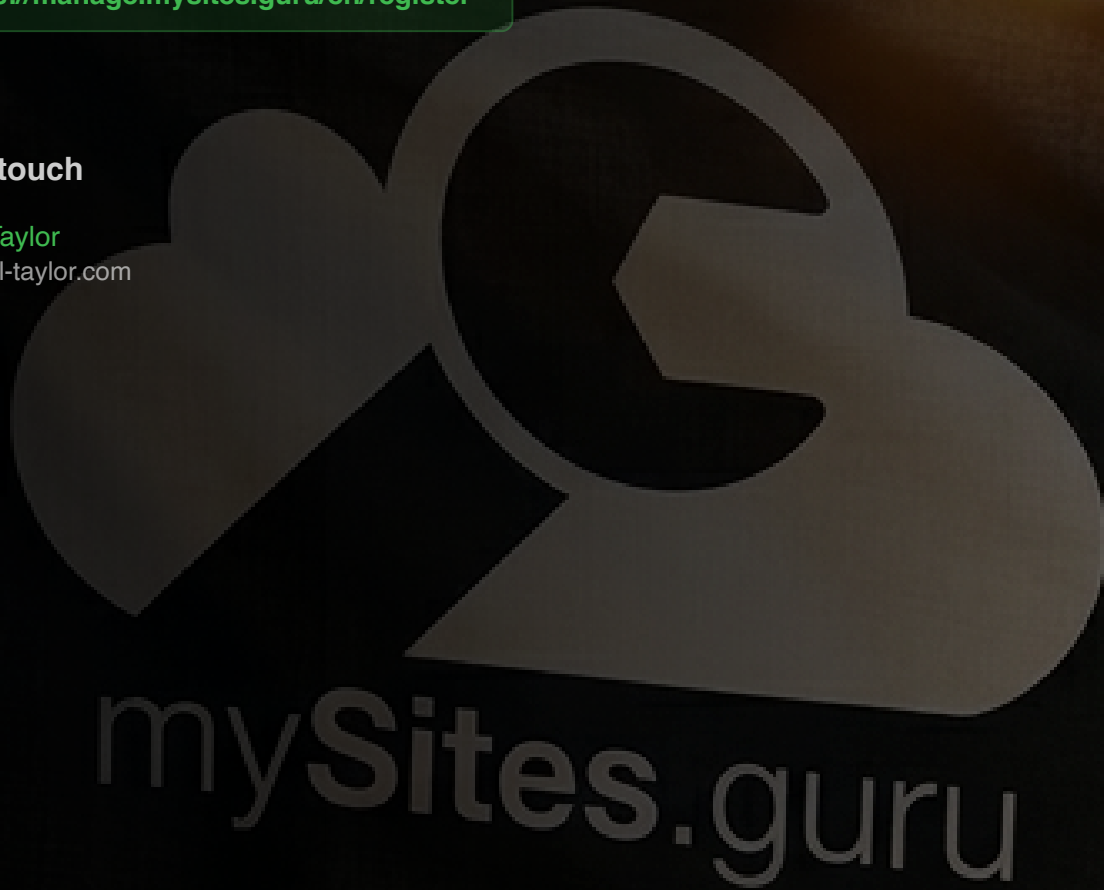
Get Your Free Site Audit

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

