



Stagelt 5.8.0 and 6.4.0 fix CSRF on every action, and a settings file that could run PHP

Stagelt 5.8.0 and 6.4.0 add CSRF protection to every staging action and stop an Options save writing PHP into params.php. Our reading, and what to do.

Phil E. Taylor | 26 October 2026

Stagelt is a Joomla extension by Barnaby V. Dixon of php-web-design.com that builds a staging copy of a live Joomla site inside a `/stageit/` folder, lets you work on the copy, and pushes it back over the live site with Sync to Live, taking an automatic backup of the live site into `/stgbackups/` before each push. On 24 October 2026 he released Stagelt 5.8.0 for Joomla 5 and Stagelt 6.4.0 for Joomla 6, and each changelog has the same Security section: a security token on every Stagelt action, backup delete and restore limited to Stagelt's own folder, a settings file that could run PHP, two cross-site scripting paths, and a bar that any visitor could switch off.

The reason this one matters is where the tool sits. A staging extension copies the whole site and can overwrite the live one, so its actions are among the most powerful buttons in the administrator area. Before these releases none of those buttons checked Joomla's security token, and one of them, saving Options, could write PHP into Stagelt's own settings file. Stagelt is also the kind of extension an agency installs for a redesign and leaves in place for years, which is the install an attacker hopes to find.

TL;DR

- Stagelt **5.x below 5.8.0** and **6.x below 6.4.0** ran every action (building, pushing, removing, restoring and deleting backups, saving Options, clearing logs) without Joomla's security token, so another website could trigger them through a logged-in administrator's browser
- A setting containing an **apostrophe could break out of** `params.php` and run as PHP; settings are now stored encoded
- On the vendor's description, those two together let a crafted page visited by a Stagelt administrator **write PHP onto the server**. We score that chain 8.6 High on CVSS 4.0 from the changelog; no CVE has been published
- Backup delete and restore **accepted any folder path**; they now act only inside `/stgbackups/`

- Two XSS paths are escaped, and switching the Stagelt bar off now needs a logged-in Stagelt administrator rather than any visitor
- Both releases came out on **24 October 2026**. 5.8.0 is the last Joomla 5 release with new features or bug fixes; that line is security-only from here, in line with Joomla 5
- This is the developer's own fix. We have not diffed or tested the code, which is commercial; our analysis is of the published changelog

8.6

CVSS 4.0

Stagelt before 5.8.0 and 6.4.0: CSRF to PHP in the settings file (no CVE)

HIGH mySites.guru assessment from the vendor changelog

A page on another website, opened by a logged-in Stagelt administrator, could submit an Options save with no token check. A setting containing an apostrophe could break out of the params.php settings file and run as PHP on the server. The same missing token check also covered push, remove, restore and backup delete, which could overwrite or remove the live site.

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

Needs a logged-in Stagelt administrator to visit a page

No login needed by the attacker

Fixed in 5.8.0 and 6.4.0

▼ 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: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

How a Stagelt Options save could become PHP on the server

Two items in the changelog describe separate fixes, and read together they describe one attack. The first is the CSRF entry: building, pushing, removing, restoring and deleting backups, saving Options and clearing logs "now require Joomla's security token, so another website can't trigger them through a logged-in administrator's browser". Each action also now accepts only its own known steps. Before the release, then, none of those actions checked the token, and saving Options was one of them.

The second is the settings file entry: "A setting containing an apostrophe could break out of the settings file (params.php) and run as PHP. Settings are now always stored safely encoded." Stagelt writes its Options into `params.php`, a PHP file, and a value with an apostrophe in it could close the string it was written into, so whatever followed ran as PHP.

Put those together and the Options screen stops being an administrator-only problem. On the vendor's own description, a page on another site visited by a logged-in Stagelt administrator could submit an Options save that writes PHP into the settings file, and that is code execution on the server. Without the CSRF, the same injection needed someone who could already save Stagelt's Options, which on most sites is the people who own it anyway. The missing token check is what hands that write to a stranger with a link.

That is the chain we scored at 8.6 High on CVSS 4.0: network attack, low complexity, no privileges for the attacker, one user interaction from the victim, and high impact on confidentiality, integrity and availability of the site. We have not built the request or run it against any site, and the vendor has not published a CVE. The score is our reading of

the two changelog entries, and we would rather tell you what they add up to than wait for someone else to.

The rest of the Stagelt 5.8.0 and 6.4.0 security fixes

The same missing token check covered push, remove and restore, so the fix for the Options save also closes a crafted page pushing the staging copy over live, removing the staging site, or restoring a backup, through an administrator who happened to be logged in. The remaining entries, worst first:

1. **Backup delete and restore accepted any folder path.** The changelog says the delete-backup and restore-backup actions "accepted any folder path sent to them", and they now act only on folders inside `/stgbackups/`. Combined with the missing token check, on the changelog's description, a crafted page could point those actions at a folder of its choosing.
2. **Two cross-site scripting paths.** The Stagelt bar's Switch to Live and Switch to Staging links, and the tab parameter on Stagelt's screens, could include script code from a crafted link. Both are now escaped, the bar decides whether it is on the staging site from the installation folder rather than from the address, and its colour settings only accept real colour values.
3. **Any visitor could switch the Stagelt bar off.** Turning the bar off now needs a logged-in Stagelt administrator. Before, it did not need a login at all.
4. **Backups were easier to find from the web.** Backup folders now get a random suffix in their name, `/stgbackups/` gets a blank `index.html` and an `.htaccess` that also works on Apache 2.4, the `robots.txt` block no longer names the backups folder, and the record of the last push can no longer be read from the web.

There is some smaller hardening alongside: the command line lock file is kept in the site's own tmp folder, table prefix matching treats `_` literally, and the Admin Tools fingerprint step ignores paths containing `..`. Both releases also add command line push and remove, through `php cli/joomla.php stageit:status`, `stageit:push`, `stageit:remove` and `stageit:backups`.

What we did and did not check

Everything above comes from the vendor's published changelogs. Stagelt is a commercial extension, so we have not diffed the before and after code, and we have not tested any of these paths on any site, live or otherwise. The severity is our assessment of what the changelog describes.

Which Stagelt versions are affected?

Stagelt 5.x below 5.8.0 and Stagelt 6.x below 6.4.0, which is where the vendor shipped the fix. There are two current lines, one per Joomla version, and each got its own release on the same day:

Joomla version	Stagelt line	Fixed in
Joomla 6	Stagelt 6	6.4.0
Joomla 5	Stagelt 5	5.8.0 (security-only line from now on)
Joomla 3 and 4 era	Stagelt 4 and older	No fix in this release; not checked

The Joomla 5 line is worth a second look. The vendor's support-status note says 5.8.0 is the last Stagelt for Joomla 5 release with new features or bug fixes; from here on it receives security releases only, in line with Joomla 5, and new features go into Stagelt for Joomla 6. So this update is also the last one that line gets that is not purely a security fix.

Of the installs mySites.guru flags for this, about 86% are on the Stagelt 5 line and about 14% on Stagelt 6. Separately, about 40% of all the Stagelt installs we see are Stagelt 4 or older, from the Joomla 3 and 4 era. Those received no fix in this release. We have not checked that older code, so we do not flag those versions, and the right way to read that is unverified, not safe.

What to do about Stagelt now

1. **Update.** Stagelt 5 sites to 5.8.0, Stagelt 6 sites to 6.4.0, and confirm the installed version afterwards.
2. **Look at the backups and the logs.** After updating, open `/stgbackups/` and the Stagelt audit log and look for pushes, restores or deletes that no one on your team ran. A push you did not make is a live site that was overwritten; a delete you did not make is a backup you no longer have.
3. **Remove it if you no longer stage.** If the redesign shipped a year ago and no one has opened Stagelt since, remove the extension and the `/stageit/` copy. A staging copy of your site is a second full install to keep patched, and one fewer powerful action set in the administrator area.
4. **Stagelt 4 or older:** there is no fixed release on that line. Move the site to a Joomla version with a current Stagelt line, or remove the extension.

How mySites.guru flags vulnerable Stagelt installs

mySites.guru added rules for this on 26 October 2026 to our [vulnerability database](#), flagging Stagelt 5.x below 5.8.0 and 6.x below 6.4.0 on every connected Joomla site. A commercial extension with no CVE and a changelog on the vendor's own site does not show up in a CVE feed, which is why we read vendor changelogs rather than wait for a record.

The flagged sites can go out in one batch with the [mass updater](#), which on this release mostly means the Joomla 5 line. That works the same way across a [portfolio of Joomla sites](#) of any size and is part of every [subscription](#).

Why Stagelt's admin actions are worth an attacker's time

Staging tools are installed for one job. An agency puts Stagelt on a site for a redesign, works on the copy for a few weeks, pushes it live, and moves on to the next client. The extension stays behind, with the power to overwrite the live site, restore an old copy over it, or delete the backups, and no one opens it again until the next redesign.

That makes its actions a high-value target for cross-site request forgery in a way that a gallery or a contact form is not. CSRF needs a victim who is logged in and a target action worth triggering, and an extension that can push a whole site over live is about as worth triggering as it gets. The administrator does not have to do anything in Stagelt, only be logged in to Joomla and open the wrong page somewhere else.

In fifteen years of looking after client sites, the extensions that cause the worst days are rarely the ones the client uses daily. They are the ones someone installed for a project, that still work, and that still have every permission they were given. If you look after Joomla sites for other people, the list of staging and migration tools left installed across them is worth an afternoon this week.

Further Reading

- [Stagelt 5 changelog](#) - the vendor's release notes for the Joomla 5 line, including the 5.8.0 Security section.
- [Stagelt 6 changelog](#) - the vendor's release notes for the Joomla 6 line, including the 6.4.0 Security section.
- [CWE-352: Cross-Site Request Forgery](#) - the weakness class behind the missing token checks.
- [CWE-94: Improper Control of Generation of Code](#) - the weakness class behind a settings file that can become PHP.
- [OWASP Cross-Site Request Forgery Prevention Cheat Sheet](#) - why a per-request token is the standard defence, and why cookies alone are not.

Frequently Asked Questions

What did Stagelt 5.8.0 and 6.4.0 fix?

Both releases add Joomla's security token to every Stagelt action (building, pushing, removing, restoring and deleting backups, saving Options and clearing logs), limit backup delete and restore to folders inside /stgbackups/, stop a setting with an apostrophe breaking out of the params.php settings file and running as PHP, escape two cross-site scripting paths in the Stagelt bar and the tab parameter, and require a logged-in Stagelt administrator to switch the bar off.

Is the Stagelt settings file flaw remote code execution?

On the vendor's own description, a setting containing an apostrophe could break out of params.php and run as PHP, and before this release saving Options had no token check. Read together, a page on another site visited by a logged-in Stagelt administrator could submit an Options save that writes PHP into the settings file. We have not tested it, so this is our reading of the changelog, not a demonstrated exploit.

Which Stagelt versions are affected?

Stagelt 5.x below 5.8.0 and Stagelt 6.x below 6.4.0, which is what mySites.guru flags. Stagelt 4 and older, from the Joomla 3 and 4 era, received no fix in this release and we have not checked that code, so treat those versions as unverified rather than safe.

Is there a CVE for the Stagelt 5.8.0 and 6.4.0 security fixes?

No CVE has been published. The 8.6 High score in this post is our own CVSS 4.0 assessment of the worst chain described in the changelog, not a vendor or CNA score.

Does Stagelt for Joomla 5 still get updates after 5.8.0?

Security releases only. The vendor's support-status note says 5.8.0 is the last Stagelt for Joomla 5 release with new features or bug fixes, in line with Joomla 5 itself. New features go into Stagelt for Joomla 6.

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

Yes. Since 26 October 2026 mySites.guru flags every connected Joomla site running Stagelt 5.x below 5.8.0 or 6.x below 6.4.0 on its dashboard, so you can update the affected sites from one place.

AI MODIFIED

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

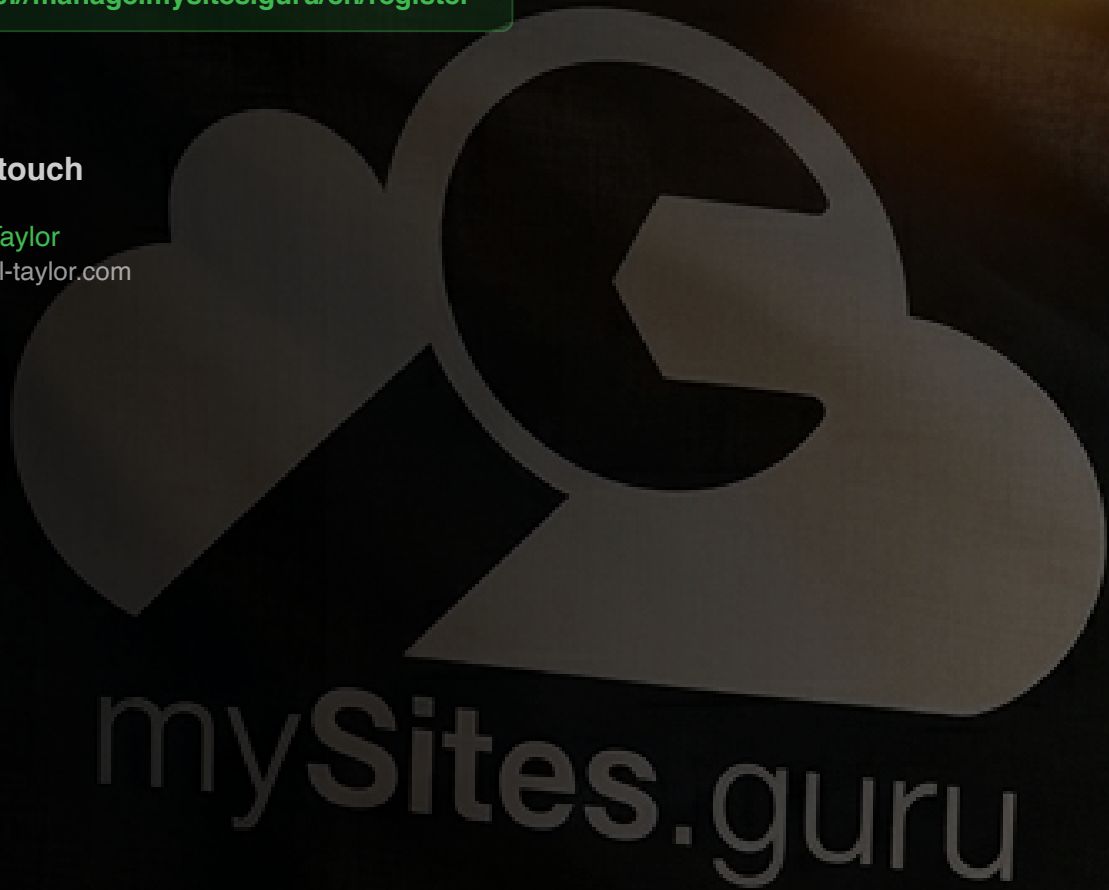
Get Your Free Site Audit

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