mySites.guru

Fabrik 4.7.2 for Joomla: A Long List of Security Fixes

Fabrik 4.7.2 for Joomla closes a long list of unauthenticated vulnerabilities, most of them found and reported by mySites.guru. Here is the full list and what to do.

Phil E. Taylor | 22 August 2026

⚠ **Active Joomla Extension security alerts:** SP Page Builder RCE • JCE 2.9.99.10 • Fabrik 4.7.2 • Phoca Cart: unauth SQLi • ZOO: unauth RCE

Do not confuse this with the earlier Fabrik updates, it is a brand-new release out today (Saturday)

Fabrik has shipped several security releases in the past fortnight, and 4.7.2 itself has been re-issued more than once under the same version number. The build that closes the full list below was released **today, Saturday 22 August 2026**. Download the latest 4.7.2 fresh from fabrikar.com, and re-download it even if a site already reports 4.7.2, because the version string alone does not tell you which build you have.

Fabrikar released **Fabrik 4.7.2** for Joomla on 22 August 2026. It is a security release, and it closes a long list of unauthenticated vulnerabilities in the application and form builder, most of them found and reported by mySites.guru and credited to us by name in Fabrik's own changelog.

If you run Fabrik on any Joomla site, update to the latest 4.7.2 build now. This post is the plain list of what it fixes and what to do. For the back-story of how the 4.7.x line got here, across 4.6.7, 4.6.8, 4.7.0 and 4.7.1, see The Fabrik Fiasco.

TL;DR

- **Fabrik 4.7.2** (22 August 2026) is a security release closing a long list of **unauthenticated** vulnerabilities: remote code execution, SQL injection, arbitrary file upload, directory listing, row disclosure, comment manipulation, path traversal and a heredoc breakout
- **Most of the fixes are credited to mySites.guru** in Fabrik's changelog
- The Joomla CNA has **published a CVE record for every one**, and **fifteen credit mySites.guru** as the finder, **four of those at CVSS 10.0**

- **Update every Fabrik install to the latest 4.7.2 build**, downloaded fresh from fabrikar.com. Re-download it even if a site already shows 4.7.2, because 4.7.2 has been re-issued more than once under the same version number
- **Joomla 3 sites cannot install any Fabrik 4 release.** There is a manual one-line vendor patch for the calc flaw, offered as-is; plan removal or migration
- mySites.guru flags every connected Joomla site running Fabrik through 4.7.2

The full list of fixes

The Joomla CNA has published a CVE record for every one of these, and **fifteen of them credit mySites.guru as the finder**, four of those at the maximum **CVSS 10.0**. They are listed here worst first, with the vendor's own description of each. Every CVE links to its published record.

CVE	CVSS 4.0	What it is	Reported by
CVE-2026-76604	10.0 Critical	Unauthenticated remote code execution via `form_php` `_runPHP`	mySites.guru
CVE-2026-76605	10.0 Critical	Unauthenticated remote code execution via the image element with the eval flag	mySites.guru
CVE-2026-76606	10.0 Critical	Path traversal in the image element	mySites.guru
CVE-2026-76607	10.0 Critical	Missing access check in the download plugin's foreign-key branch	mySites.guru
CVE-2026-77992	9.5 Critical	Heredoc escaping breakout in the calc element	mySites.guru
CVE-2026-76571	9.3 Critical	Unauthenticated SQL injection in the list filter condition parameter	mySites.guru
CVE-2026-76602	9.3 Critical	Unauthenticated SQL injection in ORDER BY, via a `CONCAT(` allowlist bypass	mySites.guru

CVE	CVSS 4.0	What it is	Reported by
CVE-2026-76596	8.7 High	Unauthenticated table truncation via `list.doempty`	mySites.guru
CVE-2026-76597	8.7 High	Unauthenticated arbitrary file upload to the web root, in the list email plugin	mySites.guru
CVE-2026-76598	8.7 High	Unauthenticated arbitrary directory listing via `onAjax_getFolders`	mySites.guru
CVE-2026-77027	8.6 High	Unauthenticated code execution via JavaScript injection in the JS-Actions regex condition	Fabrik
CVE-2026-76600	6.9 Medium	Unauthenticated deletion of any comment	mySites.guru
CVE-2026-76601	6.9 Medium	Unauthenticated row reordering in the Order plugin	mySites.guru
CVE-2026-76603	6.9 Medium	Unauthenticated row disclosure via `form.inlineedit`	mySites.guru
CVE-2026-76608	6.9 Medium	Unauthenticated disclosure of any commenter's email address	mySites.guru
CVE-2026-76609	6.9 Medium	Unauthenticated modification of any comment	mySites.guru

Fabrik 4.7.2 also re-closed a regression of the original calc-element flaw, CVE-2026-66915, which had been reachable again through a second placeholder substituter; the changelog credits mySites.guru with reporting that regression. The two remote code execution flaws that started this whole run, CVE-2026-66915 in the calc element (reported by Moe Khalilov of LeetProtect Research) and CVE-2026-67282 in the list filter model (reported by Murad Gasimov), were both scored CVSS 4.0 10.0 Critical and fixed earlier in the 4.6.x line.

Just how bad is this?

Honestly, about as bad as an extension vulnerability set gets. Four of these are scored **CVSS 10.0**, the maximum, and each of the four is reachable by an anonymous visitor with no login: two are direct remote code execution, one is a path traversal in the image element, and one strips out an access check. Add the 9.5 heredoc breakout and the two 9.3 SQL injections and that is seven Critical-rated unauthenticated flaws in a single component, before you count the Highs and the Mediums.

We have been finding and reporting Joomla extension vulnerabilities for years, and a list this long and this severe closed in one release is among the worst we have seen in a long time. If you run Fabrik, treat it that way. Any version below 4.7.2 should be assumed exposed, and the sites most at risk are the ones that publish a Fabrik form or list a visitor can reach without logging in.

What to do

1. **Update every Fabrik install to the latest 4.7.2 build.** Download it fresh from My Download Files on fabrikar.com, and re-download it even if a site already reports 4.7.2, because the package has been re-issued more than once under the same version number. It needs a valid Fabrik subscription, and Joomla's updater will not offer it at default settings, so this is a manual download and install.
2. **Test before you deploy.** 4.7.x is a real upgrade rather than a point release: it breaks any `userAjax` calls you use, and sites running the FullCalendar or Paypal plugins need those updated to current versions at the same time. Install and test on a sandbox before a live site.
3. **Joomla 3 sites need a different plan.** Fabrik 4 installs on Joomla 4.2 and above and Joomla 5.1 and above only. There is no patched Fabrik 3 release. The vendor has published a manual one-line source patch for the calc flaw in its Announcements forum, offered as-is with no warranty; apply it as a stopgap while you plan removal or migration.
4. **Check exposed sites for compromise.** An unauthenticated flaw leaves no login trail, so updating does not tell you whether a site was already hit. Look for

unfamiliar administrator accounts, recently modified or unexpected PHP files, and scheduled tasks you did not create.

Finding every Fabrik install across your Joomla sites

The hard part of a list like this is not the fix, it is finding every site that needs it before an attacker does. mySites.guru keeps a live inventory of every extension on every connected Joomla site and flags the ones running an affected version of Fabrik, so this turns into a filtered list rather than an afternoon of logging into control panels. We flag every Fabrik install through 4.7.2 while we independently verify the latest build.

At a glance

Field	Detail
Component	Fabrik for Joomla (`com_fabrik`)
Vendor	Fabrikar (fabrikar.com)
Type	Multiple unauthenticated flaws: remote code execution (CWE-94), SQL injection (CWE-89), arbitrary file upload (CWE-434), path traversal (CWE-22), directory listing and access-control failures
CVSS 4.0	Up to 10.0 (Critical). Four issues score the maximum 10.0, seven are Critical in all, the rest High and Medium
CVEs	Sixteen published by the Joomla CNA, fifteen crediting mySites.guru as finder. The full list, with links and scores, is in the table above
Impact	Unauthenticated remote code execution, full-database SQL injection, arbitrary file upload to the web root, and unauthorised disclosure or modification of data, most with no login, token or user interaction
Finder	Phil Taylor, mySites.guru (fifteen of the sixteen)
Affected versions	Every Fabrik release below 4.7.2

Field	Detail
Fixed in	Fabrik 4.7.2, released 22 August 2026

Further Reading

- The Fabrik Fiasco: Announced, Restricted, Relabelled, the back-story across 4.6.7 to 4.7.0
- Fabrik's changelog history, the vendor's own record of the fixes
- CVE-2026-66915 and CVE-2026-67282 at CVE.org, the two originally published remote code execution flaws
- Every security announcement we have published, the full archive, which this release joins
- AJAX endpoints are a big CMS security blind spot, the pattern behind most of the flaws in the list above
- Twenty rules for Joomla extension developers handling a security report, the standard this release is measured against

Frequently Asked Questions

What is Fabrik 4.7.2?

Fabrik 4.7.2 is a security release of the Fabrik application and form builder for Joomla, published by Fabrikar on 22 August 2026. It closes a long list of unauthenticated vulnerabilities across the calc element, list filters, the image element, the comment and order plugins, and more. Most of the fixes are credited to mySites.guru in the vendor's own changelog. Every Fabrik version below 4.7.2 should be treated as affected.

Which vulnerabilities does it fix?

Fabrik's changelog for 4.7.2 lists fixes for unauthenticated remote code execution in the calc and image elements, unauthenticated SQL injection in the list filters and ORDER BY handling, an unauthenticated arbitrary file upload to the web root, an unauthenticated directory listing, unauthenticated disclosure, modification and deletion of comments, an unauthenticated row disclosure and reordering, a path traversal and a heredoc escaping breakout. The full table is in this post. Most carry no login, no token and no user interaction.

Are these CVEs published?

Yes. The Joomla CNA has published a CVE record for every one of these, and fifteen of them credit mySites.guru as the finder, four of those at the maximum CVSS 10.0. Each CVE in the table below links to its published record.

Which are the most serious?

Four are scored CVSS 4.0 10.0 Critical: CVE-2026-76604 and CVE-2026-76605 are unauthenticated remote code execution, CVE-2026-76606 is a path traversal in the image element, and CVE-2026-76607 is a missing access check in the download plugin. CVE-2026-77992, the heredoc escaping breakout in the calc element, is 9.5, and the two SQL injections, CVE-2026-76571 and CVE-2026-76602, are 9.3. All of them are unauthenticated.

How do I update, and can every site take it?

Download the latest 4.7.2 build fresh from fabrikar.com and install it. Re-download it even if a site already reports 4.7.2, because 4.7.2 has been re-issued more than once under the same version number. Fabrik 4 installs on Joomla 4.2 and above and Joomla 5.1 and above only. Joomla 3 sites cannot install any Fabrik 4 release and there is no patched Fabrik 3

release; the vendor has published a manual one-line source patch for the calc flaw for Fabrik 3, offered as-is, and you should plan removal or migration for those sites.

How do I find every Fabrik install across my Joomla sites?

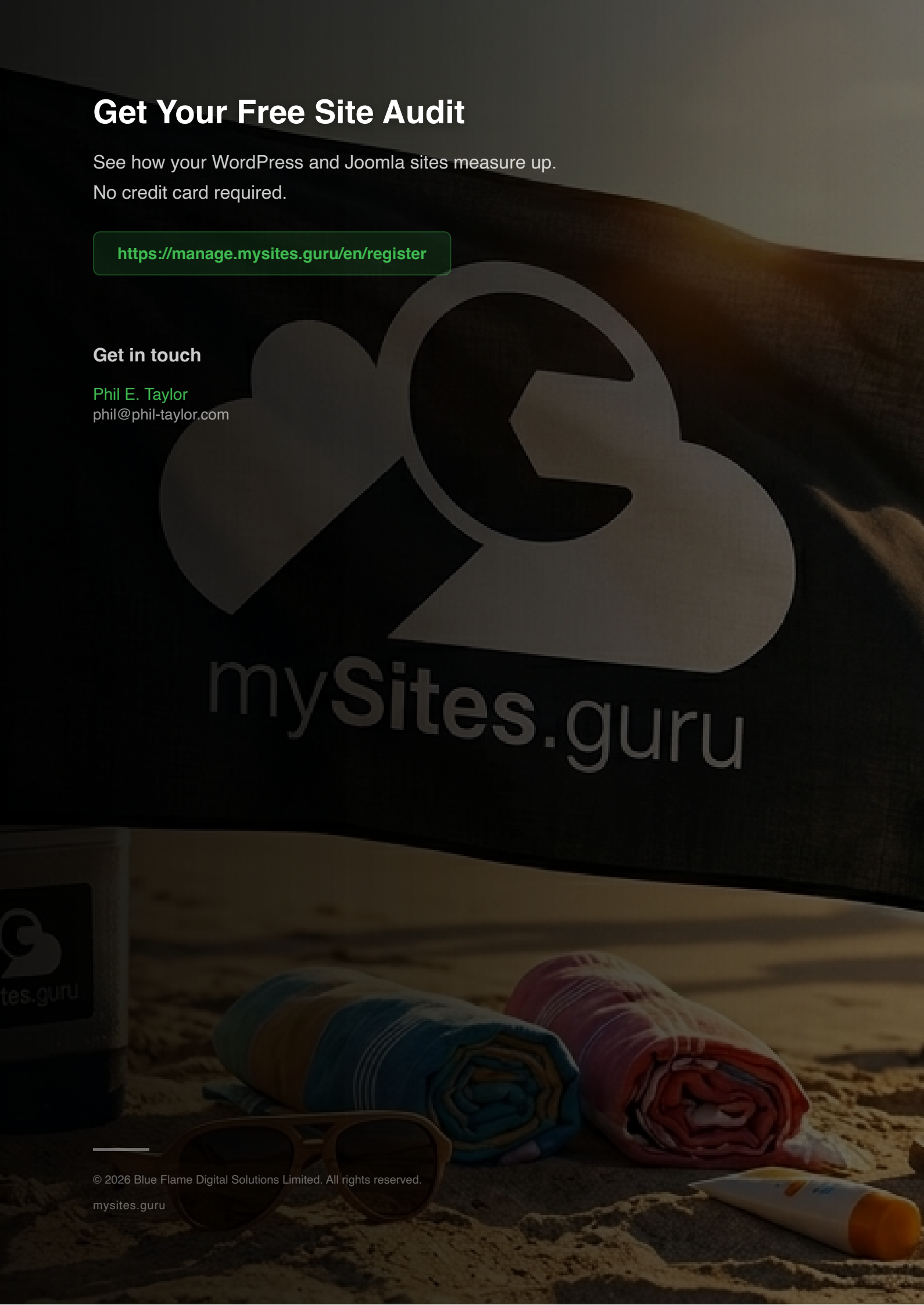
mySites.guru keeps a live inventory of every extension on every connected Joomla site and flags the ones running an affected version of Fabrik, so you get a filtered list rather than checking each site by hand. It flags every Fabrik install through 4.7.2 while we independently verify the latest build.

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