Fix Joomla 3 Security Issues in One Click

Patch every known Joomla 3 security vulnerability across all your sites with a single toggle in mySites.guru - no manual file edits, no eLTS subscription.

Phil E. Taylor | 25 March 2026

Joomla 3 is end of life. The official project stopped releasing public updates at 3.10.12, but new vulnerabilities keep turning up. In January 2025 alone, three more were disclosed via the eLTS programme.

Manually patching 55 files per site is tedious enough when you have five sites. When you have five hundred, forget it.

mySites.guru fixes every known Joomla 3 security issue with a single click.

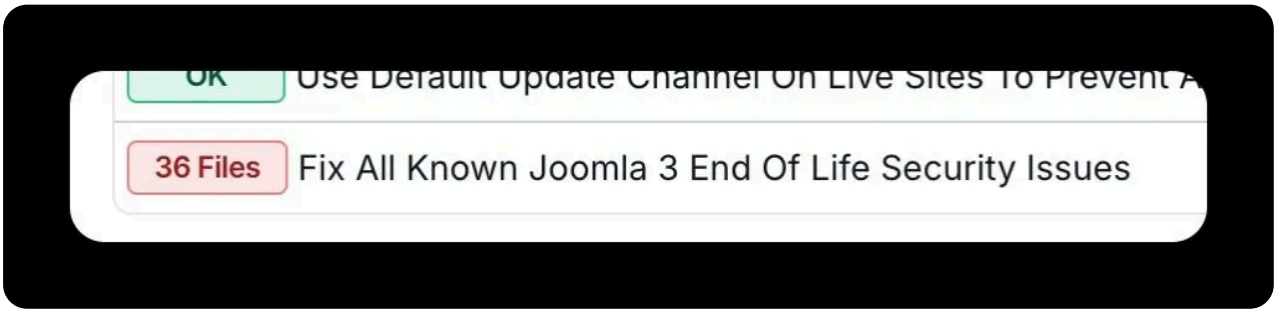
> *"We include all Joomla 3 security fixes in the service. No eLTS subscription needed."*

How Does It Work?

The patch tool is in the Site Snapshot for each Joomla 3.10.12 site in your mySites.guru account. One toggle. That's it.

Under the hood, the mySites.guru connector tracks the MD5 hash of each file that needs patching. Flip the toggle on and it compares hashes against the expected patched versions, replacing anything that doesn't match. Flip it off and the files revert to stock 3.10.12.

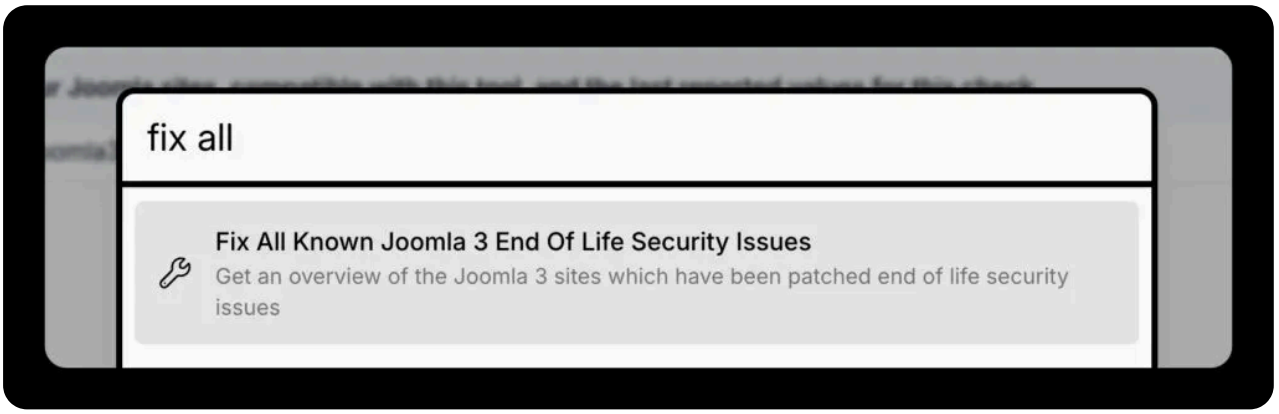
The tool only runs on Joomla 3.10.12, the last publicly released version of the Joomla 3 series. It ignores the commercial eLTS programme entirely.



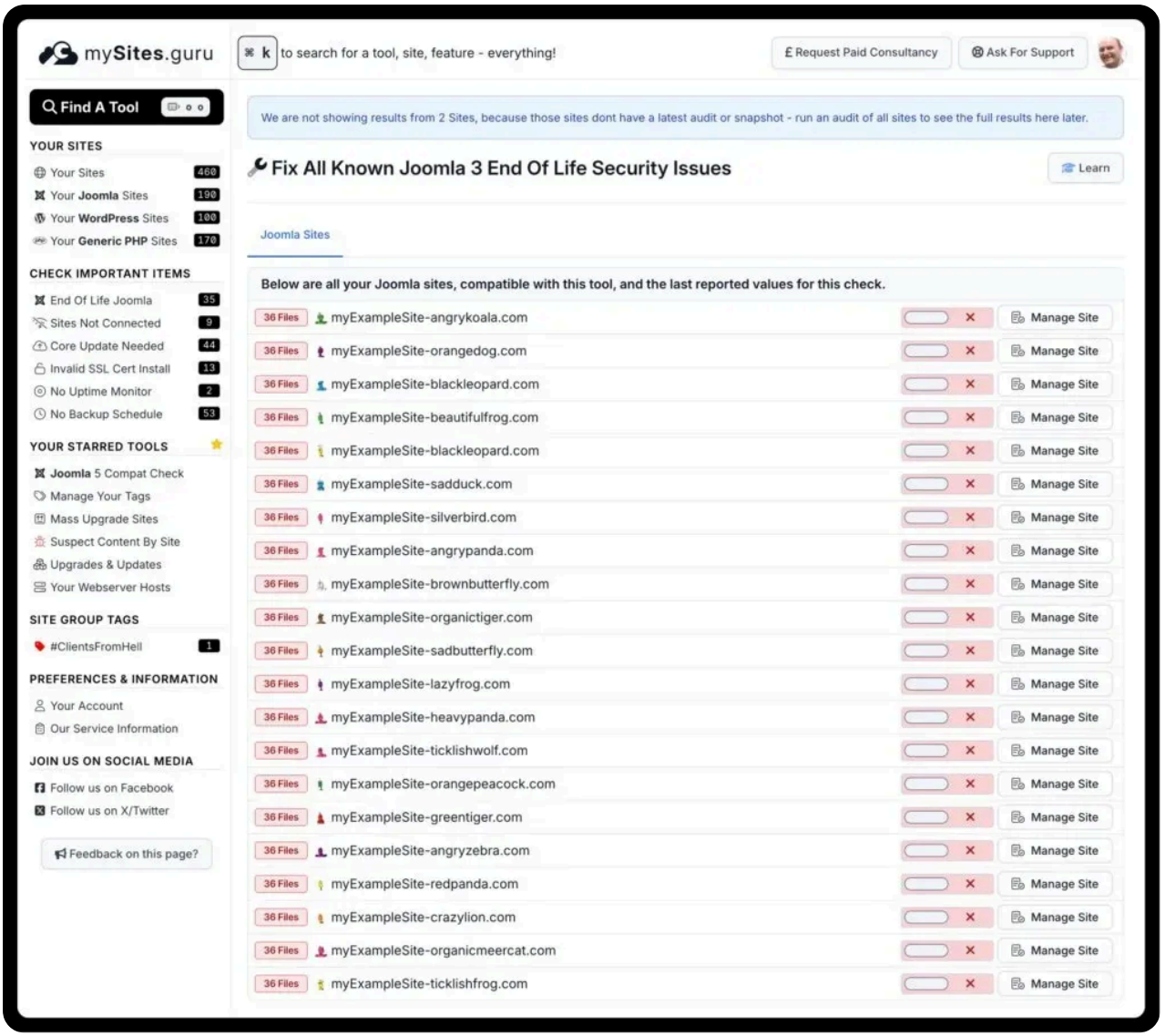
Where Do You Find the Tool?

Two ways to get there:

1. Cmd+K and search for “Fix All Known Joomla 3”
2. Open your site’s Snapshot and scroll to the Joomla Configuration section



Both paths lead to a tool overview page listing every Joomla 3.10.12 site you manage, along with each site’s current patch status.



How Do You Patch Multiple Sites at Once?

Got dozens or hundreds of Joomla 3 sites? Click the grid icon next to the toggle to open the bulk view. It shows every Joomla 3.10.12 site with individual toggles. If you're managing multiple Joomla sites from a single dashboard, this bulk view is where you'll spend most of your time.

Direct link:
manage.mysites.guru/en/tools/allsites/Joomla/joomlaconfiguration/joomla3eol

What vulnerabilities does it fix?

Individually, none of these will get your site hacked while you sleep. But stacked together across an unpatched site, they add up. The patch covers 55 files and addresses every known vulnerability disclosed since 3.10.12:

XSS vulnerabilities

- CVE-2024-21724 - XSS in media selection fields
- CVE-2024-21725 - XSS in mail address outputs
- CVE-2024-21726 - Inadequate content filtering within the filter code
- CVE-2024-21731 - XSS in StringHelper::truncate method
- CVE-2024-26278 - XSS in com_fields default field value
- CVE-2024-26279 - XSS in Wrapper extensions
- CVE-2024-40743 - XSS vectors in Outputfilter::strip* methods
- CVE-2024-40747 - XSS vectors in module chromes
- CVE-2024-40748 - XSS vector in the id attribute of menu lists

Other vulnerabilities

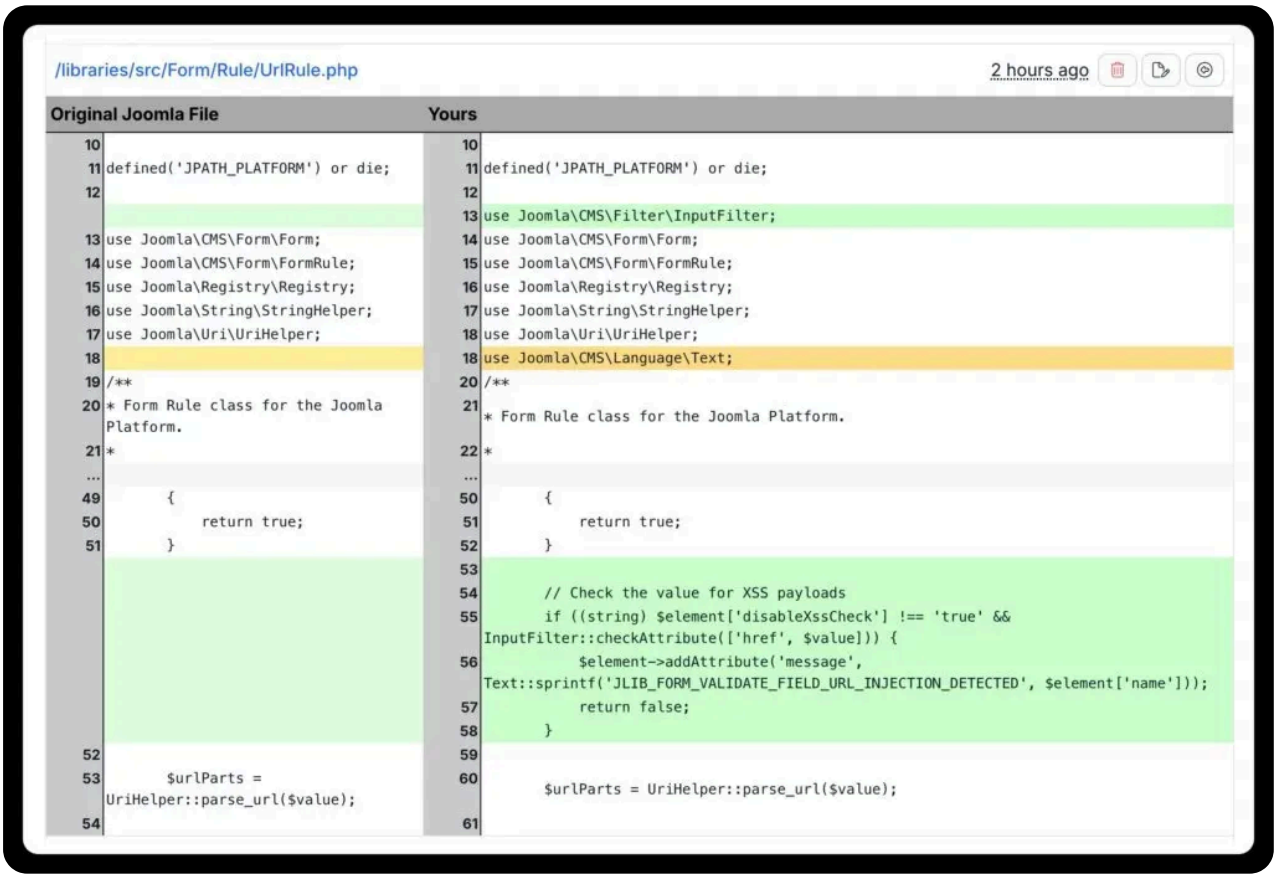
- CVE-2024-27184 - Inadequate validation of internal URLs
- CVE-2024-27185 - Cache poisoning in pagination
- CVE-2024-21723 - Open redirect in installation application
- CVE-2024-21722 - Insufficient session expiration in MFA management views
- CVE-2023-40626 - Exposure of environment variables
- CVE-2024-40749 - Read ACL violation in multiple core views

eLTS bug-fix-for-bug-fix patches

- Fixes in 3.10.19-elts that repair broken code shipped in 3.10.18-elts
- Fixes in 3.10.18-elts that repair broken code shipped in 3.10.17-elts

How Do Patched Files Show Up in Audits?

After patching, your mySites.guru audit will flag the modified files as Core File Changes, because they *are* changes to the original 3.10.12 distribution. You can inspect every diff directly in the audit tool.



Which Files Does the Patch Modify?

The tool patches 55 files: a mix of PHP files (the actual security fixes) and XML form definitions (tighter input validation). You need both. Changing the XML alone isn't enough.

▼ Full list of patched files (55 files)

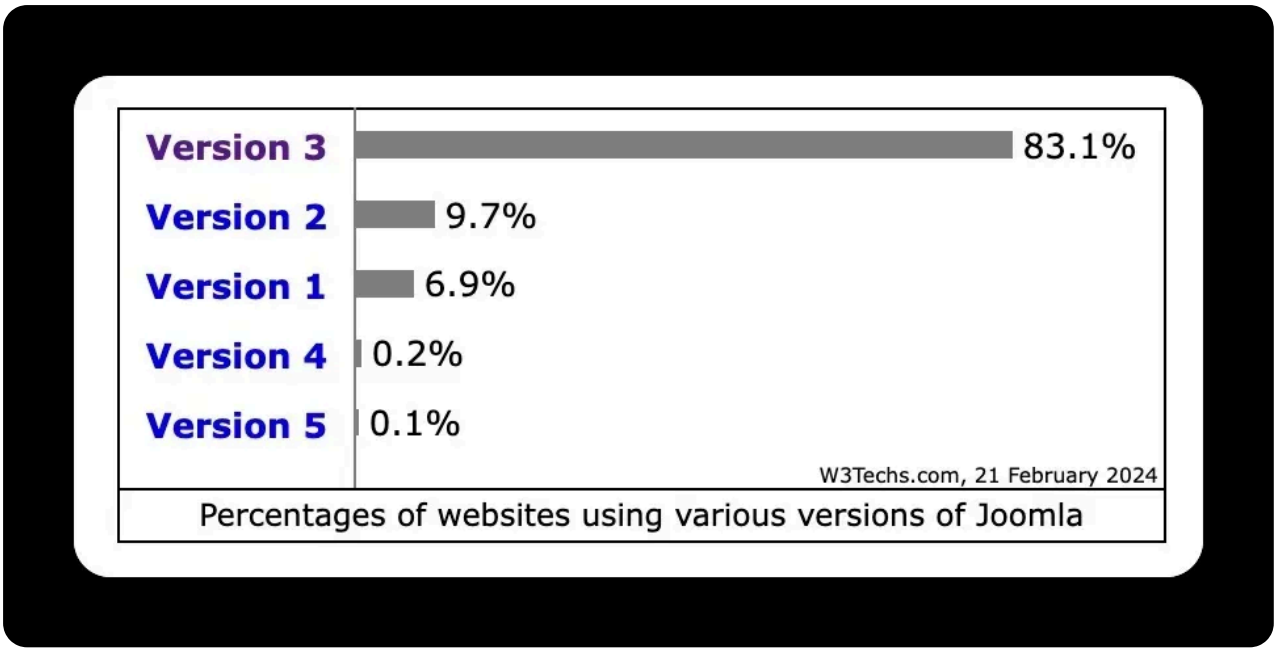
- administrator/components/com_config/model/form/application.xml
- administrator/language/en-GB/en-GB.com_config.ini
- components/com_content/views/archive/view.html.php
- components/com_finder/views/search/view.html.php
- components/com_search/views/search/view.html.php
- libraries/src/Cache/Cache.php
- libraries/src/Pagination/Pagination.php
- administrator/components/com_banners/models/forms/banner.xml
- administrator/components/com_categories/models/forms/category.xml
- administrator/components/com_contact/config.xml
- administrator/components/com_contact/models/forms/contact.xml
- administrator/components/com_content/models/forms/article.xml
- administrator/components/com_fields/models/forms/field.xml
- administrator/components/com_menus/models/forms/item_alias.xml

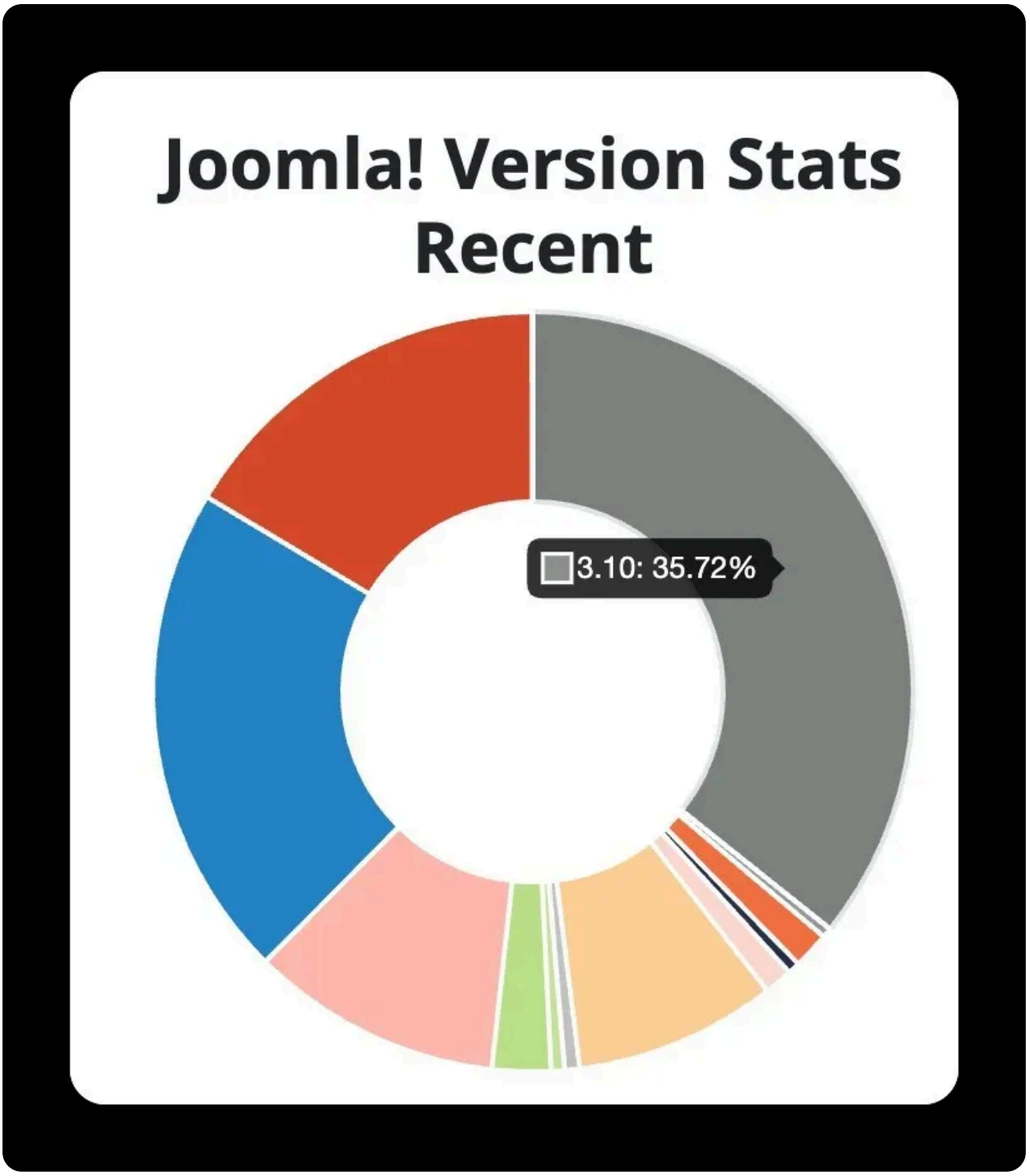
- administrator/components/com_menus/models/forms/item_component.xml
- administrator/components/com_menus/models/forms/item_heading.xml
- administrator/components/com_menus/models/forms/item_separator.xml
- administrator/components/com_menus/models/forms/item_url.xml
- administrator/components/com_menus/models/forms/itemadmin_alias.xml
- administrator/components/com_menus/models/forms/itemadmin_component.xml
- administrator/components/com_menus/models/forms/itemadmin_container.xml
- administrator/components/com_menus/models/forms/itemadmin_heading.xml
- administrator/components/com_menus/models/forms/itemadmin_url.xml
- administrator/components/com_newsfeeds/models/forms/newsfeed.xml
- administrator/components/com_tags/models/forms/tag.xml
- administrator/components/com_users/models/user.php
- administrator/language/en-GB/en-GB.lib_joomla.ini
- administrator/templates/hathor/templateDetails.xml
- administrator/templates/isis/templateDetails.xml
- components/com_content/models/forms/article.xml
- components/com_tags/views/tag/tmpl/default.xml
- components/com_tags/views/tag/tmpl/list.xml
- components/com_tags/views/tags/tmpl/default.xml
- components/com_users/models/profile.php
- components/com_users/views/login/tmpl/default.xml
- components/com_wrapper/views/wrapper/tmpl/default.xml
- includes/framework.php
- libraries/cms/html/string.php
- libraries/fof/download/adapter/cacert.pem
- libraries/src/Form/Rule/UrlRule.php

- libraries/src/Http/Transport/cacert.pem
- libraries/src/Language/LanguageHelper.php
- libraries/src/Uri/Uri.php
- libraries/vendor/joomla/filter/src/InputFilter.php
- libraries/vendor/joomla/filter/src/OutputFilter.php
- modules/mod_custom/mod_custom.xml
- modules/mod_wrapper/mod_wrapper.xml
- plugins/user/profile/profile.php
- templates/beez3/templateDetails.xml
- templates/protostar/templateDetails.xml
- components/com_privacy/controller.php
- components/com_privacy/privacy.php
- components/com_users/controller.php
- components/com_users/users.php
- modules/mod_menu/tmpl/default.php

Why Does Joomla 3 Still Matter?

Joomla 3 is still everywhere. W3Techs shows version 3 running on the majority of Joomla installations, and Joomla's own usage statistics put 3.10.x at over 35% of reporting sites.


Version 3
83.1%
Version 2
9.7%
Version 1
6.9%
Version 4
0.2%
Version 5
0.1%
W3Techs.com, 21 February 2024
Percentages of websites using various versions of Joomla



If you run a digital agency, you already know: migrating clients from Joomla 3 to 4 or 5 takes budget, developer time, and client sign-off. That doesn't happen overnight, and the sites still need protecting in the meantime.

What Is the Joomla 3.10.999 Project?

The patches in mySites.guru come from the open-source Joomla 3.10.999 project. That repo has every Joomla 3.10 version from 3.10.12 onwards, plus diffs for all patches released under the commercial eLTS programme.

Same approach as the earlier Joomla 1.5.999 and Joomla 2.5.999 repos. It'll be maintained for as long as Joomla 3 sites exist.

Stop patching files by hand

If you're still running Joomla 3, stop tracking CVEs by hand. Add your sites to mySites.guru, flip the toggle, and get on with your day.

The broader picture of securing Joomla and WordPress sites is covered in the WordPress and Joomla security guide. For Joomla-specific agency workflows, see the Joomla agency handbook.

Start your free trial →

Frequently Asked Questions

Can I fix Joomla 3 security vulnerabilities without manually editing files?

Yes - mySites.guru provides a one-click toggle in the Site Snapshot that automatically patches all known Joomla 3 security issues across your sites.

How many files does the mySites.guru Joomla 3 patch tool modify?

The tool currently modifies 55 files to address all known security vulnerabilities since Joomla 3.10.12 was released.

What types of security issues does the Joomla 3 patch tool fix?

It addresses XSS vulnerabilities, cache poisoning, inadequate URL validation, insufficient session expiration, and exposure of environment variables, among others.

Do I need a Joomla eLTS subscription to get these patches?

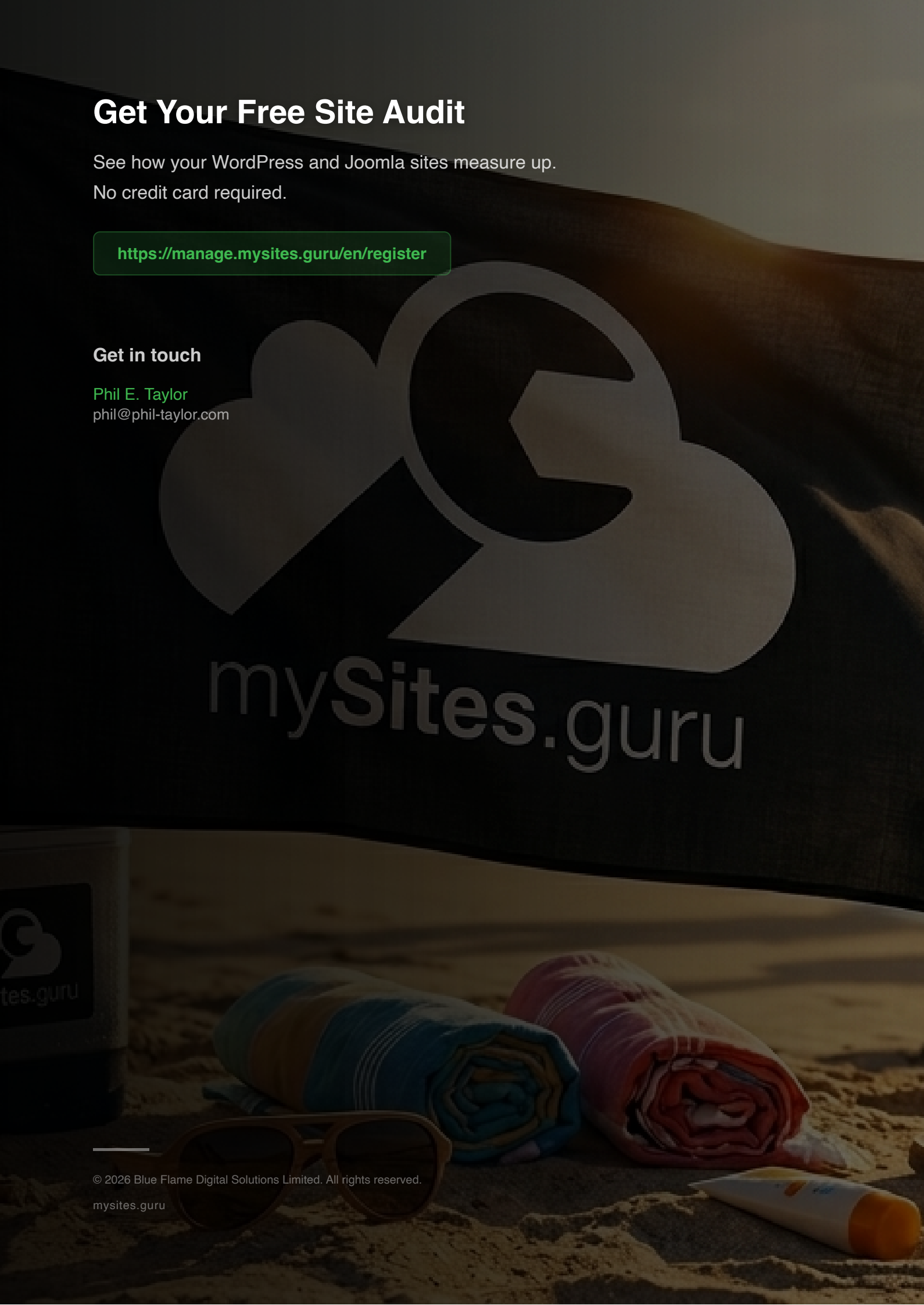
No. mySites.guru includes all known Joomla 3 security patches as part of your subscription - no separate eLTS licence required.

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