



Helix Ultimate 2.2.11 Is a Security Release. Its Download Page Doesn't Say So.

Helix Ultimate 2.2.11 fixes XSS, path traversal and CSRF issues in 2.0.0 to 2.2.10, and its download page doesn't say so. What changed and how to update.

Phil E. Taylor | 29 October 2026

~~TL;DR~~: JoomShaper released Helix Ultimate 2.2.11 on 29 October 2026. It is a security release, rated Moderate by the vendor, fixing XSS, path traversal and CSRF issues in every version from 2.0.0 to 2.2.10. You would not know that from the download page, which gives a version number, a date and three Download buttons, or from the GitHub release notes, which never use the word. The most significant fix corrects the embed filter that 2.2.10 introduced as a security fix: it had Joomla's InputFilter flags backwards. Every fix needs a logged-in user with some edit rights. Updating is a two-part job, because Joomla Updates offers the framework plugin but not the template. There is no Joomla 3 version. Across the Joomla 4, 5 and 6 sites we monitor on the 2.2.x line, about 90 percent were on 2.2.10 when this was released.

Helix Ultimate is a Joomla template framework from JoomShaper, installed as the `helixultimate` system plugin plus the `shaper_helixultimate` template. It renders the whole front end of a site, so a security release for it is worth acting on rather than filing, and this one needs a little more care than the 2.2.10 release did, because half of it does not come through the Joomla updater.

Nothing on the Download Page or the Release Notes Says Security

The Helix Ultimate download page on joomshaper.com shows "Version 2.2.11 · Released 29 Oct 2026 · Joomla 6, 5, 4", a QuickStart button, and three packages (Quickstart Pack Joomla 6, Template, Plugin) with Download buttons. There is no severity, no affected range, and no advice to update. A site owner who checks the page before deciding whether to bother this week has no reason to hurry.

The GitHub release notes are the same. They list twenty pull requests, every one titled "Fix:" or "Feat:", and the word "security" does not appear in them. The six security pull requests (#566, #570, #571, #574, #578, #580) were merged on GitHub on 19 October 2026, ten days before the release, in the public repository, so the fixes themselves sat in the open for over a week before anyone could install them.

To be fair to JoomShaper, the announcement exists. A post in the JoomShaper Community Facebook group is titled "Important Security Update: Helix Ultimate v2.2.11 Is Here!" and says the release has "security fixes to help protect your Joomla website against potential vulnerabilities, including XSS, path traversal, and CSRF issues". It gives a severity (Moderate, CVSS around 6.5), an affected range (2.0.0 to 2.2.10), the fixed version, and the supported Joomla versions (4.4.x, 5.x and 6.x). The repository's CHANGELOG.md, added in this release, also has a Security section listing six items. The information is all there, in places most site owners do not check. The places they do look, the download page and the release notes, read like a maintenance release.

No CVE has been assigned yet. The issues are not in CISA's Known Exploited Vulnerabilities list, and JoomShaper has not said they are being exploited.

What Helix Ultimate 2.2.11 Fixes

Six security pull requests, worst first:

Fix	Who can reach it	What changed
Embed filter (#580)	Anyone who can edit an article	The media tag list was being treated as a block list; it is now a strict allow-list
Media picker (#574)	A template editor using the Helix media picker	Folder names, file names, paths, preview URLs and breadcrumbs are now escaped
Error page preset (#578)	An administrator editing template style settings	The preset name is limited to letters, numbers, underscore and hyphen, otherwise "default"
Mega Menu badge (#571)	A menu editor	Badge text is filtered as a plain string and stripped of tags
Blog image removal (#566)	An article editor	Rejects an article id of 0 or less, and any image the article does not reference

Fix	Who can reach it	What changed
Article rating (#570)	Site visitors (a bug, not a hole)	The JavaScript now sends the token the server already demanded; range and published checks added

The Embed Filter Was Running Backwards

Helix Ultimate renders a blog article's audio and video embeds through

`Helper::sanitizeEmbed()` (the changelog calls it `sanitizeMediaCode`). The audio embed field is a free-text box saved with no filtering (`filter="raw"`), set by anyone who can edit the article, and `sanitizeEmbed` is the only thing between that box and the page.

In 2.2.10, `sanitizeEmbed` passed Joomla's InputFilter a list of six media tags (`iframe` , `audio` , `video` , `source` , `a` , `img`) and a list of attributes, with the mode flags set to `1, 1`. In Joomla's InputFilter, `0` means "only allow these" and `1` means "only block these". So the list meant to be the only tags allowed was the list removed, and everything else fell back to Joomla's generic built-in block list. The six media tags the feature exists to render were stripped, and anything the generic list does not know about was passed through. 2.2.11 passes `0, 0, 0` : a strict allow-list, which is what the code was always meant to be.

2.2.10 was itself the fix for the embed issue later published as [CVE-2026-78077](#), a stored XSS in the Mega Menu layout container and embed inputs. That fix went out with its filter inverted and stayed that way for two months.

Why JoomShaper's Own Test Passed

2.2.10 ships a security test, `tests/security/Phase05XssSanitizeTest.php`, that checks "sanitizeEmbed should preserve allowed iframe tags". That is the right check. It runs against a stand-in for Joomla's InputFilter in `tests/security/bootstrap.php`, a `JoomlaInputFilterStub` whose `getInstance()` ignores the two mode flags and always treats the list as an allow-list.

So the test passed against code that, on a real Joomla site, strips iframes. The stub could not tell `1, 1` from `0, 0` because it does not read the flags. In 2.2.11 the standard's signature was changed to take optional parameters, and it still ignores them, so the test still cannot distinguish the broken call from the fixed one. The fix is real; the test that would stop it regressing is not there yet.

Media Picker Escaping

The framework's own media picker built its HTML from folder names, file names, paths, preview URLs and breadcrumbs without escaping any of them. 2.2.11 runs them all through `htmlspecialchars`. Reaching it needs access to the Helix media picker in the template editor, so whoever could abuse it is already a template editor.

Error Page Preset Name

The template's `error.php` built a stylesheet path from the template's saved preset name. 2.2.11 only accepts letters, numbers, underscore and hyphen in that name and otherwise falls back to "default". This is the "path traversal" in the announcement. The value comes from the template style settings, which only an administrator can change, so it is a reasonable hardening of a path an administrator could already influence.

Mega Menu Badge Text

Badge text on a Mega Menu item is now run through Joomla's InputFilter as a plain string, then stripped of tags. It needs menu edit rights. The same pull request fixed a broken SQL condition, a missing closing parenthesis, in the query multilingual sites use to find the home template style.

Blog Image Removal

The handler that removes a blog image from an article now rejects an article id of 0 or less, and will not remove an image the article does not reference. This tightens the same code path as [CVE-2026-78075](#), which Phil Taylor of mySites.guru reported in August 2026 and which was fixed in 2.2.10 and J3 Security Fixes 1.0.3. On the Joomla 4, 5 and 6 line this handler only edits the article's own settings and never deletes a file,

so the change here is hardening. We did not report any of the 2.2.11 issues; this was JoomShaper's own work.

The "CSRF" Fix Is a Rating Bug

The announcement lists CSRF, and the pull request behind it is titled "resolve article rating invalid token issue". It is a bug fix to a feature the CSRF protection had already broken. 2.2.10's rating handler checked Joomla's form token on the server with `Session::checkToken()`, but the template's JavaScript never sent one, so every rating from a visitor was rejected with "Invalid Token". 2.2.11 makes the JavaScript send the token, and adds checks that the rating is between 1 and 5 and that the article is published.

So the CSRF protection was already on the server, and this release made the rating feature work with it while tightening the validation. Useful, but no hole was closed.

Who Can Actually Exploit These?

Someone with a login. Every security fix in 2.2.11 needs an authenticated user with some edit rights: an article editor for the embed filter and the blog image handler, a menu editor for the badge text, a template administrator for the media picker and the error page preset. We found nothing in the diff that an anonymous visitor can reach, which is the difference between this release and 2.2.10, where one item needed no account at all.

JoomShaper rates it Moderate, CVSS around 6.5, and we agree it is not an emergency. It is worth doing this week, because the plugin half is a one-click update and the embed fix restores the only filter between an article editor's raw embed box and every page that renders that article.

How Do I Update Helix Ultimate to 2.2.11?

In two parts, and the second one is the part people miss. Helix Ultimate installs as two pieces: the "System - Helix Ultimate Framework" plugin (element **helixultimate**), which Joomla Updates offers, and the Helix Ultimate template (**shaper_helixultimate**), which does not appear in Joomla Updates and has to be downloaded from JoomShaper and installed by hand. Updating the plugin alone leaves the template on 2.2.10.

1. Take a backup. The framework renders your entire front end and a bad update is visible to every visitor.
2. Log in to the Joomla administrator, go to **System**, then **Update**, then **Extensions**, and update the System - Helix Ultimate Framework plugin to 2.2.11.
3. Go to the Helix Ultimate download page on joomshaper.com and download the **Template** package. This is the one for an existing site; it keeps your content.
4. Install it through **System**, then **Install**, then **Extensions**.
5. Clear the Joomla cache.

Do not install the QuickStart Pack on a live site. It is a whole new demo site, not an update, and the download page puts it first.

Update Helix Ultimate on every site in one go

The mySites.guru Mass Extension Updater lists every site where the Helix Ultimate Framework plugin has 2.2.11 waiting and updates them all from one screen. For the template half, the Mass Package Installer takes JoomShaper's Template zip once and installs it on every site you tick.

[See the Mass Extension Updater →](#)

What About Joomla 3 Sites?

Nothing in 2.2.11 reaches them. The release is for Joomla 4.4, 5 and 6 only. Joomla 3 sites run [JoomShaper's separate Joomla 3 security build](#), which reports version 2.1.4-j3sec, and JoomShaper has not said whether the 2.2.11 fixes will be backported to it.

If you look after Joomla 3 sites on Helix Ultimate, [our write-up of that build](#) covers how it is delivered and why those sites cannot tell from their own version number whether they have it.

How Many Sites Have Updated So Far?

Very few, so far.

About 90%

were on 2.2.10 when 2.2.11 was released

Joomla 4, 5 and 6 sites we monitor running the 2.2.x framework plugin

Under 4%

had moved to 2.2.11 within the first hour

Same sites, measured against the plugin version each reports

Figures are from the mySites.guru extension inventory on 29 October 2026 and cover the framework plugin, which is the half Joomla Updates offers.

The 90 percent figure is the good news: on the current 2.2.x line, the 2.2.10 security release did get installed over the two months it had. The same installs now need the plugin update and the template package, and the template half will not move on its own.

Finding Every Helix Ultimate Install in One Place

Searching for an extension across a lot of Joomla sites by hand means logging into each administrator and reading the Manage screen, twice over for a release that updates a plugin and a template separately.

mySites.guru keeps a live inventory of every extension, template and framework on every connected Joomla site, so you can search for Helix Ultimate once and see every site and the version each one reports. It flags the plugin and the template separately, so

a site where only the plugin was updated still shows as needing the template. The vulnerability rule for 2.2.11 went live today. One of our customers said in the same Facebook thread that they had updated Helix on over 100 websites in three minutes with mySites.guru.

If a site turns out to be compromised rather than only out of date, patching will not clean it. fix.mysites.guru handles that for a single fixed fee of GBP 120 per incident, usually same day.

The Bottom Line

Helix Ultimate 2.2.11 is a security release that does not look like one from the two places a site owner checks. The announcement in the Facebook group is clear and the changelog in the repository is accurate; the download page and the GitHub release notes say nothing. The fixes themselves are sound, the most important of them corrects a security fix from August that had its filter flags inverted, and all of them need a logged-in user to reach.

Update the plugin through Joomla Updates, then install the Template package by hand, on every Joomla 4, 5 and 6 site running the framework. Leave the QuickStart Pack alone. There is no Joomla 3 build yet. If you want to see which of your sites are still on 2.2.10, on either half, start with a [free audit](#) on one of them.

Further Reading

- [Helix Ultimate v2.2.11 on GitHub](#) - the release tag and its twenty pull requests.
- [Helix Ultimate 2.2.10](#) - the previous security release, whose embed fix this one corrects.
- [JoomShaper's third Joomla 3 security patch](#) - the separate Joomla 3 build, and why those sites cannot tell whether they have it.

- Helix Ultimate 2.2.7 - the security release before that, from July 2026.
- JoomShaper on joomla3security.com - the Joomla 3 security builds JoomShaper maintains.

Frequently Asked Questions

What is Helix Ultimate 2.2.11?

A release of the Helix Ultimate template framework for Joomla 4.4, 5 and 6, published by JoomShaper on 29 October 2026. JoomShaper announced it in its Community Facebook group as a security update fixing XSS, path traversal and CSRF issues, rated Moderate (CVSS around 6.5), affecting every version from 2.0.0 to 2.2.10. It also contains a batch of Joomla 6 compatibility fixes and a few new options.

Is Helix Ultimate 2.2.11 urgent?

Not an emergency, but worth doing this week. Every security fix in the release needs a logged-in user with some edit rights (an article editor, a menu editor or a template administrator), and we found nothing in the diff that an anonymous visitor can reach. The plugin half is a one-click update, so there is little reason to leave it.

How do I update Helix Ultimate to 2.2.11?

In two parts. The System - Helix Ultimate Framework plugin updates through System, then Update, then Extensions in the Joomla administrator. The template (shaper_helixultimate) does not appear there: download the Template package from JoomShaper's download page and install it through System, then Install, then Extensions. Updating the plugin alone leaves the template on 2.2.10. Do not install the QuickStart Pack on an existing site; it is a whole new demo site.

Does Helix Ultimate 2.2.11 apply to Joomla 3 sites?

No. 2.2.11 is for Joomla 4.4, 5 and 6 only. Joomla 3 sites run JoomShaper's separate Joomla 3 security build, which reports version 2.1.4-j3sec, and 2.2.11 does nothing for them. JoomShaper has not said whether the 2.2.11 fixes will be backported.

Did mySites.guru find the security issues fixed in 2.2.11?

No. These were JoomShaper's own work. The one connection is the blog image removal fix, which tightens the same code path as [CVE-2026-78075](#), reported by Phil Taylor of mySites.guru in August 2026 and fixed in 2.2.10 and J3 Security Fixes 1.0.3. On Joomla 4, 5 and 6 that handler only edits the article's own settings and never deletes a file, so the 2.2.11 change there is hardening.

Is there a CVE for Helix Ultimate 2.2.11?

Not yet. No CVE has been assigned, the issues are not in CISA's Known Exploited Vulnerabilities list, and JoomShaper has not said they are being exploited. The six security pull requests were merged in the public repository on 19 October 2026, ten days before the release.

Why did JoomShaper's own test not catch the embed filter problem in 2.2.10?

Because the test runs against a stand-in for Joomla's InputFilter that ignores the two mode flags and always treats the tag list as an allow-list. The real InputFilter treats a flag of 1 as a block list, so the test passed against code that, on a real Joomla site, stripped the iframes the test said it kept. The stand-in in 2.2.11 still ignores the flags.

Why is the CSRF fix in 2.2.11 described as a rating bug?

Because the server already checked Joomla's form token on article ratings in 2.2.10. The template's JavaScript never sent one, so visitors' ratings were rejected with Invalid Token. 2.2.11 makes the JavaScript send the token and adds checks that the rating is between 1 and 5 and the article is published. The protection was already there; this release made the feature that depends on it work.

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

mySites.guru

© 2026 Blue Flame Digital Solutions Limited. All rights reserved.

mysites.guru