mySites.guru

Digital Peak patches four Joomla extensions after a Claude audit

Digital Peak shipped out-of-band fixes for DPCalendar, DPMedia, DPAttachments and DPCases on 10 September. DPAttachments is the one to do first.

Phil E. Taylor | 10 September 2026

Digital Peak shipped five releases across four Joomla extensions today, all rated High and all out of band. The vendor puts eleven of the twelve fixes down to a security analysis run with Claude over the last few days. The twelfth is the DPCalendar location title, which we reported on 27 August and which the announcement now credits to us.

That is the third DPCalendar security release in nine weeks, and the first one that reaches past the calendar into the rest of the catalogue. The code is public for three of the four extensions, so we read the actual changes rather than working from the severity ratings.

> **Do DPAttachments first, then the rest**
>
> DPAttachments 5.8.1 is the only one the vendor asks you to prioritise, and the code shows why: the attachment download route checked that an attachment record existed and never checked whether the person asking was allowed to have it. The other three generally need an account, or content arriving from a source you already trust.

TL;DR

- Five releases: **DPCalendar 10.12.1** and **8.19.6**, **DPMedia 1.21.1**, **DPAttachments 5.8.1** and **DPCases 3.8.1**. Every one of them is tagged Security: High on its download page
- **DPAttachments is the priority.** Unpublished attachments, attachments on a restricted view level, and attachments outside their publish window could all be downloaded by someone with no entitlement to them
- The releases are **out of band**. Digital Peak normally ships on the fourth Thursday of the month, and today is the second Thursday
- **The Joomla 3 branch got one fix, not three.** DPCalendar 8.19.6 is security only and its release notes list the unescaped location title alone

- **The DPCalendar fix is one we reported.** We sent it to Digital Peak and the Joomla Security Strike Team on 27 August, and the vendor's announcement now credits it
- **Eleven of the twelve have no CVE yet.** The DPCalendar location title is the exception, under CVE-2026-78071, whose affected range was widened on release day to take in 10.12.0 and 8.19.5
- Two of the fixes share a shape worth recognising: in both DPAttachments and DPCalendar, the escaping was already present on the field next door and simply missing on one
- **DPCalendar is not one update.** On release day our Release Radar recorded 59 distinct DPCalendar items moving to the new versions

What did Digital Peak fix on 10 September?

Twelve issues across four extensions, four of them rated High and eight Medium. The vendor's announcement lists them by severity, and each release page lists the internal tracker numbers.

Extension	Fixed in	High-severity issue	Also fixed
DPCalendar	10.12.1, 8.19.6	Location title not escaped in the map view and upcoming module	Microsoft and Exchange attachment filename hardening, CSRF state parameter on calendar imports
DPMedia	1.21.1	DPReferences shows references to users without media manager access	Path traversal on external file names, Google Drive search injection, OAuth state parameter, two permission plugin fixes
DPAttachments	5.8.1	Unauthorised access to direct downloads	Stored XSS in the CSV preview, upload context validation
DPCases	3.8.1	User information not escaped in views	Path traversal for icons outside the root

The DPCalendar row is the one with a history. That flaw is the tail of an incomplete fix from the previous release, and we are the ones who reported it, which is covered further down.

Digital Peak states that none of the twelve allows a file to be placed on the server, and that there is no evidence of exploitation in the wild. We found nothing to contradict that. There is no public proof-of-concept and no exploit code for any of them.

Two items in the DPMedia release notes are worth flagging because they do not appear in the announcement's security list at all: a permission plugin that should check delete and save, and a restricted adapter that should consider permissions from the category and the article. Both read as access-control work. Neither is described as a security fix.

DPAttachments 5.8.1 is the update to do first

DPAttachments is developed in a fully public repository, so this one can be read rather than inferred. The fix for the High-severity issue is a single commit, `Case 12252: Check access if an attachment can be downloaded`.

Before the fix, the download controller looked up the attachment by the ID in the request and made one check:

```
 public function download(): void
 {
    $attachment = $this->getModel()->getItem($this->input->get('id'));
-   if (!\is_object($attachment)) {
+   if (!$attachment instanceof \stdClass || !$this->app->bootComponent('c
        header('HTTP/1.0 404 Not Found');
        exit(0);
    }
```

The original test asks whether the attachment exists. It does not ask whether the requester is entitled to it. Those are different questions, and only one of them was being asked.

The fix adds a `canView()` method to the component and calls it from both the download controller and the front-end attachment view, which had the same gap:

```
public function canView(\stdClass $attachment): bool
{
    if ($this->canDo('core.edit', $attachment->context, $attachment->item_
        return true;
    }

    $user = $this->app->getIdentity();
    if ($user === null || (int)$attachment->state !== 1) {
        return false;
    }

    if (!\in_array((int)$attachment->access, $user->getAuthorisedViewLeve
        return false;
    }

    $now = (new Date())->toSql();

    if (!empty($attachment->publish_up) && $attachment->publish_up > $now)
        return false;
    }

    return empty($attachment->publish_down) || $attachment->publish_down >
}
```

Read that as a list of the things that were not being enforced, because that is what it is. Publication state, view access level, publish-up date and publish-down date were all recorded on the attachment and none of them governed who could download it.

The acceptance tests added alongside the fix say the same thing more bluntly. One is titled `canNotOpenUnpublishedAttachmentDetailsPage`, and its stated intent is “that an unpublished attachment cannot be viewed by a guest”. A test written to assert that a guest cannot do something is a test written because a guest could.

This is the classic missing-authorisation shape, CWE-862, and it is the same pattern we wrote up when Events Booking exposed invoices and when Cotton Cloud patched the login and left the data. Attachment IDs are sequential integers, which is the part that turns a missing check into a practical problem.

We are describing the mechanism at the level the vendor did, and not publishing a request template, because most sites running this extension have not updated yet.

The escaping was already there, one field along

The second DPAttachments fix, `Case 12253`, is in the CSV preview template. It escaped the body of the table and not the header row.

```
 <?php foreach ($csv->titles as $title) { ?>
-    <td><?php echo $title; ?></td>
+    <td><?php echo $this->escape((string)$title); ?></td>
 <?php } ?>
 <?php foreach ($csv->data as $row) { ?>
     <?php foreach ($row as $value) { ?>
-        <td><?php echo nl2br(htmlentities((string) $value)); ?></td>
+        <td><?php echo nl2br($this->escape((string)$value)); ?></td>
     <?php } ?>
```

The data cells were already running through `htmlentities()`. The header cells, four lines above them in the same file, were not. Digital Peak committed a test fixture, `test-xss.csv`, whose first column heading is a working `<script>` tag, and an acceptance test that asserts the script does not execute.

The DPCalendar fix has the same signature. In the location map template, the description was escaped and the title beside it was not:

```
-         data-title="<?php echo $this->location->title; ?>"
+        data-title="<?php echo $this->escape($this->location->title); ?>"
         data-description="<?php echo $this->escape($description); ?>"
```

We reported that line on 27 August, six hours after 10.12.0 shipped, and it is the only DPCalendar item in this release that did not come from the vendor's own audit.

That is a pattern worth being able to spot in your own code. A defended field sitting next to an undefended one is much harder for a human reviewer to catch than a block with no escaping at all, because the visible `escape()` call on the neighbouring line makes the whole section read as handled. Anyone who has reviewed a template at the end of a long day has skimmed past exactly this.

If you have overridden any of these templates, your override still contains the unescaped output, and updating the extension will not touch a copy sitting in your template folder. That is the single most likely way to install this update and stay vulnerable, and it applies to the DPCalendar location templates for the second release running.

What changed in DPMedia and DPCases

DPMedia is half readable. The shared library and two of its plugins ship in a public repository; the DPReferences panel and the Google Drive and Dropbox providers do not, so the High rests on the vendor's description. DPCases has no public repository at all.

The DPMedia High is `DPReferences shows references for users without media manager access`, an information disclosure: the references panel listed items to people who had no business seeing the media library. The two fixes that can be read are the path traversal and the OAuth state parameter. The traversal fix adds a `resolvePath()` method that walks a virtual path segment by segment and throws when a `..` would climb above the adapter root, then routes the locally cached copy of a remote file through it, so a filename reported by a remote provider cannot steer the cache write outside `/images/dp<provider>/media`. The OAuth fix checks a `state` value against a `dp_state` cookie with `hash_equals()` before storing a refresh token, which is the standard defence against a forged callback completing an account connection the site owner never started. The same control appears in DPCalendar in this release, so the audit found it missing in two places and both were closed together.

One DPMedia fix is in the code and not in the announcement. The OAuth callback used to redirect to whatever URL the `dp_url` cookie held, and 1.21.1 adds a `getSafeRedirectUrl()` guard that falls back to `index.php?option=com_media` unless the target is relative or on the current host. That is an open redirect closed without being named as one.

The DPCases High escapes user information in views, and a second fix stops icon paths escaping the root directory. DPCases 3.8.1 also contains one feature change, support for a template images folder for icons, so it is not a security-only release.

The DPCalendar CSRF fix is the one worth understanding structurally. Adding a state parameter to an OAuth-style import flow is the standard defence against a forged request completing an account connection that the site owner never started. It appears in both DPCalendar and DPMedia in this release, which suggests the audit found the same missing control in two places and both were closed together.

Why did the Joomla 3 branch only get one of the fixes?

DPCalendar 8.19.6 is labelled security only, and its release notes list exactly one item: the unescaped location title. The package bears that out. Diffing the shipped 8.19.5 and 8.19.6 archives, and setting aside version numbers in the manifests, the entire release is one changed line of executable code. The two Medium fixes in 10.12.1, the Microsoft and Exchange filename hardening and the CSRF state parameter, are not there.

That is a defensible call and it is worth being clear-eyed about what it means. Digital Peak keeps DPCalendar 8.x in what it has called hybrid maintenance mode for Joomla 3, and it is one of the few vendors still backporting anything to a branch whose CMS reached end of life in August 2023. Compare that with JoomShaper ending Joomla 3 security fixes or J2Store 3 stopping in October and Digital Peak looks generous.

The practical reading for anyone still on Joomla 3 is that a security-only branch gets the issues the vendor rates High and not the hardening that goes with them. Every Medium

in this release is a Joomla 4, 5 and 6 fix. If a Medium is later reclassified, or turns out to be reachable in some unexpected way, the Joomla 3 branch does not have it.

Where the DPCalendar fix came from

DPCalendar 10.12.0 shipped on the morning of 27 August and fixed a location title XSS reported by Toan Le, escaping nine `data-title` sinks across the component. It left the tenth, in the location map subtemplate that the location detail page loads by default. We read the release the same afternoon, confirmed the leftover sink against a clean 10.12.0 install, and reported it to Digital Peak and the Joomla Security Strike Team six hours after the release went out.

Allon Moritz confirmed it the next morning and said the fix would ship in about a month, on the grounds that planting the payload needs DPCalendar location create permission. It arrived thirteen days later, inside this batch.

Today's announcement went up without a credit. We wrote to Digital Peak the same morning, having diffed both packages to confirm the sink was closed, and the line was added a few hours later: "Again thanks to Phil Taylor from mysites.guru for rechecking the latest release and finding the issue in the map view." Allon Moritz had been ill, and this is a vendor with a good record on attribution: it named Toan Le in August and credited us properly when we reported an unauthenticated SQL injection in July.

The other eleven issues are not ours and we make no claim on them.

The upcoming module held seven more of the same line

The changelog reads "map view and upcoming module", and the second half is the larger number. The upcoming module is a separate free download, so its packages can be diffed too. Every one of its seven layouts held the identical unescaped sink, and 10.12.1 closes all seven:

```
-   data-title="<?php echo $location->title; ?>"
+   data-title="<?php echo htmlentities($location->title, ENT_COMPAT, 'UTF
```

`blog.php`, `default.php`, `horizontal.php`, `icon.php`, `panel.php`, `simple.php` and `timeline.php`, each echoing a location title straight into a double-quoted attribute. We reported one instance, in the component; the release closed eight. Whether the other seven came out of the audit or out of someone grepping the codebase after our report is not something we can tell from the outside. Either way, if you run the upcoming module, which layout you picked made no difference.

The CVE record moved on release day

The location title flaw already had a number. CVE-2026-78071 was published on 28 August for Toan Le's original report, and its affected range stopped at 8.19.4 and 10.11.2. That range declared 8.19.5 and 10.12.0 clean, and those were the two builds still holding the missed sink.

We raised it with the Joomla CNA on the morning of the release and the record was updated within the hour. The affected range now reads 7.0.0-8.19.5 and 9.0.0-10.12.0, and the credits list two finders instead of one.

A site sitting on 10.12.0 could read the old record, conclude it was already patched, and have no reason to install 10.12.1. We follow the affected range a CVE states rather than overriding it, so our own database did not flag those sites while the record called them clean. Widening the range was the fix for that, rather than working around it.

How Digital Peak found these issues

The other eleven came out of the audit, and the vendor is unusually direct about the method. The announcement opens: "We made some security analysis with Claude in the last days and are shipping today fixes for these issues."

The findings resulted in shipped code with tests attached. Whatever the discovery method, the DPAttachments commits are public, the missing access check is visible in the diff, and the acceptance tests encode the behaviour that was wrong. That is a

higher bar than most vulnerability reports clear, and it is the bar that matters when you are deciding whether to interrupt your afternoon.

This is a long way from the first AI-assisted credit in the Joomla world. When Joomla 5.4.6 and 6.1.1 patched ten security issues in May 2026, three of those advisories credited "Doyensec in collaboration with Claude and Anthropic Research": CVE-2026-40383, CVE-2026-40384 and CVE-2026-48896. We wrote at the time that more attributions like that should be expected, and they arrived. Yannick Gaultier of weeblr credited AI tooling for two 4Analytics CVEs in July and said security audit runs would be systematic from then on, and Roland Dalmulder of RolandD Cyber Produksi described finding flaws the same way in the Joomla Community Magazine in August.

What is unusual here is the placement rather than the method: Digital Peak put it in the title of the release announcement.

Our own position on where AI sits in this work is set out in full, and it has not changed: every one of the vulnerabilities we have disclosed was found by a human reading source code first, with tooling behind it and AI used at the end to check that nothing was missed. Digital Peak has taken a different route to the same destination. Both produced patched code, which is the only output a site owner can actually use.

The code and the downloads went public together

The three DPAttachments fixes were written on 7 September, with commit timestamps between 08:33 and 09:49 UTC. They did not become public then. They reached the public repository in a push at 03:17 UTC on 10 September, and the DPCalendar Free 10.12.1 commit followed at 03:42 UTC, hours before the announcement went up.

That ordering is the right one. A public fix commit is a map to the flaw it fixes, and pushing the code days ahead of the release would have given anyone watching the repository a head start on every unpatched site. Digital Peak held the commits and published the code and the downloads together.

It also means the diff-to-exploit clock started this morning, for everybody, at the same time. That window is measured in hours now, which is the argument against leaving this until the weekend.

DPCalendar is not one update

DPCalendar ships as a component plus a large family of separately installable plugins and modules: payment plugins for Stripe, PayPal, Mollie, Braintree and Bexio, calendar integrations for Google, Microsoft, Exchange, CalDAV, Zoom, Eventbrite and more, plus map, mini, counter and upcoming modules. Each one gets its own version bump in a release like this.

On the day of this release, our Release Radar recorded **59 distinct DPCalendar items** moving to the new versions, 29 on the 10.12.1 branch and 30 on 8.19.6. A given site only needs the pieces it has installed, and most sites run a handful. But a site with several calendar integrations has a list to work through, and Joomla's update manager will present them as separate rows.

Two of those plugins matter more than the rest in this release. The Microsoft and Exchange plugins are the ones the attachment filename hardening applies to, so if you sync a calendar from a Microsoft 365 account, those are the two to check are actually on the new version rather than assuming the component update covered them.

Release Radar is free and needs no account, which is the point of it: an out-of-band release from a commercial vendor is exactly the event that no extension directory records.

How many of the sites we can see are still vulnerable?

We record the installed version of every extension on every connected site, which lets us say something about how a release like this actually spreads instead of guessing. Counting only sites that have reported in during the last 30 days, measured on the morning of release:

- **About nine in ten** DPCalendar installs are on a version below 10.12.1 or 8.19.6. That is ordinary for release day, and it is why we mail affected customers rather than waiting for someone to notice a version badge change
- **Roughly one in seven** is on the 8.x branch, and five in six of those really are running Joomla 3 underneath
- **About one in eighteen** is on the 9.x line or older, where no patch exists at all. Those sites need a staged major upgrade rather than an update, and they have been in that position since July
- DPMedia, DPAttachments and DPCases show up on far fewer connected sites than DPCalendar, few enough that quoting a percentage would imply a precision the sample does not have. Treat those three as “check whether you have them” rather than as a trend

We are not publishing site counts. The proportions are the useful part, and the size of the estate is not ours to hand out.

One more figure worth having, because it is the opposite of what the four-extension headline suggests: only about **one Digital Peak site in seventy** runs more than one of these four extensions. The stacking happens at account level instead, where roughly **one affected account in twelve** holds more than one of the products. This is a job for the agency owner with several clients, not a job that piles up on any one site.

How fast did the last DPCalendar release spread?

We can measure this one instead of guessing, because DPCalendar 10.12.0 shipped only two weeks ago. Of the sites that took that update through mySites.guru:

- Half were patched within **a day and a bit**, and just under half were done inside the first 24 hours
- **Around nine in ten** were done within three days
- **More than nine in ten of those updates were somebody clicking update.** Only about one in fourteen came from the automatic update engine

One figure should decide how you plan today, if any of your sites are still on Joomla 3:

- DPCalendar updates targeting the **8.x branch succeeded 67% of the time**. The same operation on the 10.x line succeeded **91% of the time**. Roughly one Joomla 3 update attempt in three ends stuck on a failure rather than on a patched site

That gap is the practical cost of running extensions on an end-of-life CMS, and it compounds: a failed update leaves the site unpatched, and it stays that way until someone checks. If your Joomla 3 sites matter, budget time to confirm 8.19.6 actually installed rather than assuming the click worked.

These adoption figures only see updates run through mySites.guru, and only since April 2026, so read every one of them as a floor rather than a total.

How do you update a four-extension wave safely?

The mechanics are ordinary Joomla extension updates. The parts worth care on this particular release:

1. **Start with DPAttachments 5.8.1.** It is the one with a missing authorisation check, and the only one the vendor singles out
2. **Check your branch, not the highest version number.** On Joomla 3 your DPCalendar target is 8.19.6, not 10.12.1. The 9.x line has no patch at all and needs the staged route across to 10.x
3. **Update the plugins, not just the component.** Especially the Microsoft and Exchange calendar plugins, and any payment plugins you run
4. **Check your template overrides.** If you have overridden the DPCalendar location templates or the DPAttachments CSV preview, the unescaped output is still sitting in your override and the update will not reach it
5. **Take a backup first**, particularly on the 9.x line where this is a staged upgrade rather than a point release
6. **Turn on automatic updates** so the next out-of-band release arrives without you watching for it. We wrote up how to enable auto-updates for any Joomla extension

Point four is the one that catches people. An override is a copy, and a security fix in a vendor template never reaches a copy.

How do I find every site running a Digital Peak extension?

Searching the extension by name in the mySites.guru Extension Inventory lists every connected site running it, with the version each one reports, so you work through one list instead of logging into sites one at a time to check. For a release touching four products, that is the difference between an afternoon and a morning.

Sites running a version below the fix get flagged automatically once the vulnerability is in our database, and the announcement list puts the urgent ones in your inbox on the day rather than the week after. If you are not a subscriber, the free audit will tell you what a single site is running.

The official Joomla Vulnerable Extensions List will almost certainly not record this release, which is why we keep our own vulnerability database.

Timeline

2026-08-27 — **mySites.guru reports the missed sink**

DPCalendar 10.12.0 ships that morning and escapes nine data-title sinks in the component. It leaves the tenth, in the location map subtemplate that the location detail page loads by default. We confirm the leftover sink against a clean 10.12.0 install and report it to Digital Peak and the Joomla Security Strike Team six hours after the release.

2026-08-28 — **Digital Peak confirms the report**

Allon Moritz confirms it the next morning and says the fix will ship in about a month, on the grounds that planting the payload needs DPCalendar location create permission.

2026-09-07 — **Digital Peak writes the DPAttachments fixes**

The three DPAttachments security commits are authored between 08:33 and 09:49 UTC, each named for the internal case number that later appears in the changelog. They stay private for three days.

2026-09-10 ● **The code is pushed to the public repositories**

The DPAttachments fixes reach the public repository in a push at 03:17 UTC, with the repository recording further activity at 03:34 UTC and the DPCalendar Free 10.12.1 commit at 03:42 UTC. The code and the downloads became public together rather than the code going first.

2026-09-10 ● **Digital Peak publishes the advisory and ships five releases**

DPCalendar 10.12.1 and 8.19.6, DPMedia 1.21.1, DPAttachments 5.8.1 and DPCases 3.8.1, out of band and outside the vendor's normal fourth-Thursday schedule. The announcement credits security analysis done with Claude and names each issue with a severity.

2026-09-10 ● **The CVE range is widened and the credit added**

CVE-2026-78071 is updated to cover 7.0.0-8.19.5 and 9.0.0-10.12.0, the two builds that still held the missed sink, and lists a second finder. Digital Peak adds a line to its announcement crediting mySites.guru for the map view issue.

2026-09-10 ○ **No CVE for the other eleven**

The announcement identifies the remaining issues only by internal tracker numbers. Assignment through the Joomla CNA commonly follows a release by several days.

Further Reading

- Digital Peak's own announcement - the vendor's write-up, and the source for every severity rating quoted here.
- DPCalendar 10.12.0 fixes an SQL injection and an XSS - the August release, two weeks before this one, and the reason the location title fix looks familiar.

- The unauthenticated SQL injection we found in DPCalendar in July - the flaw to check first if you have not updated since June.
- Events Booking for Joomla exposes personal and financial data from invoices - the same missing-access-check pattern as the DPAttachments download flaw, in a different extension.
- We are not the only ones auditing Joomla extensions - the wider pattern this release fits into.
- Twenty Rules for Joomla Extension Developers Handling a Security Report - the published standard a release like this can be measured against.
- CWE-862: Missing Authorization, CWE-79: Cross-site Scripting and CWE-22: Path Traversal - the standard references for the three weakness classes in this release.

Frequently Asked Questions

What did Digital Peak fix on 10 September 2026?

Twelve security issues across four Joomla extensions, four of them rated High. DPCalendar 10.12.1 and 8.19.6 fix an unescaped location title. DPMedia 1.21.1 fixes a permission check on DPReferences, a path traversal, a Google Drive search injection and a missing OAuth state parameter. DPAttachments 5.8.1 fixes unauthorised access to direct downloads, a stored cross-site scripting flaw in the CSV preview, and upload context validation. DPCases 3.8.1 escapes user information in views and blocks path traversal for icons.

Which Digital Peak update should I do first?

DPAttachments 5.8.1. It is the only one of the four where the vendor singles out the issue as needing priority, and the reason is that the attachment download route checked that an attachment existed without checking whether the person asking was allowed to have it. Unpublished attachments, attachments on a restricted view level, and attachments outside their publish window were all reachable. The other three generally need an account or content from a trusted source.

Did an AI really find these Joomla extension vulnerabilities?

Eleven of the twelve, yes. Digital Peak says so in its own announcement: 'We made some security analysis with Claude in the last days and are shipping today fixes for these issues.' The twelfth, the DPCalendar location title, came from a human: mySites.guru reported it to Digital Peak and the Joomla Security Strike Team on 27 August 2026 and the vendor confirmed it the next morning. The findings are real in the sense that matters most, which is that they resulted in shipped code changes with tests attached, all of which can be read in the vendor's public repositories. This is not the first AI-assisted credit in the Joomla world, and not close. Three Joomla core advisories fixed in May 2026 credit 'Doyensec in collaboration with Claude and Anthropic Research', covering CVE-2026-40383, CVE-2026-40384 and CVE-2026-48896. In the extension world, weeblr credited AI tooling for two 4Analytics CVEs in July 2026, and RolandD Cyber Produksi described the same method in the Joomla Community Magazine in August 2026.

Is there a CVE for these Digital Peak issues?

One of the twelve has one. The DPCalendar location title flaw is covered by CVE-2026-78071, published on 28 August 2026 for Toan Le's original report and updated on 10 September to widen the affected range to 7.0.0-8.19.5 and 9.0.0-10.12.0 and to list a

second finder. The other eleven have no CVE at the time of writing: Digital Peak's announcement names them by internal tracker number only. Assignment through the Joomla CNA often follows a release by several days, so the absence of a CVE today is a paperwork gap rather than a verdict on severity, and it is not evidence that no CVE will ever be assigned.

Who found the DPCalendar location title flaw?

Two reporters, in two stages. Toan Le found the original, which Digital Peak fixed in DPCalendar 10.12.0 on 27 August 2026 under CVE-2026-78071. That release escaped nine data-title sinks in the component and missed the tenth, in the location map subtemplate. mySites.guru reported the missed one to Digital Peak and the Joomla Security Strike Team six hours later the same day, the vendor confirmed it on 28 August, and it shipped in 10.12.1 and 8.19.6 on 10 September. Digital Peak's announcement credits it and the CVE record now lists both finders.

Why did the Joomla 3 branch only get one of the DPCalendar fixes?

DPCalendar 8.19.6 is described as security only, and its release notes list a single item: the unescaped location title. The two Medium items in 10.12.1, the Microsoft and Exchange attachment filename hardening and the CSRF state parameter on calendar imports, are not in the Joomla 3 release notes. Digital Peak still backports High-severity fixes to a branch running on a CMS that reached end of life in August 2023, which is more than most vendors do, but a security-only branch is a narrower promise than a supported one.

How do I find every site running a Digital Peak extension?

Search the extension by name in the mySites.guru Extension Inventory and every connected site running it is listed with the version each one reports. That matters more than usual for this release, because DPCalendar is not one installable item. Version reporting across every connected site is part of the mySites.guru subscription.

How many separate updates does a DPCalendar site actually need?

More than one. DPCalendar ships as a component plus a large family of separately installable plugins and modules, and each of them gets its own version bump. On the day of this release our Release Radar recorded 59 distinct DPCalendar items moving to 10.12.1 or 8.19.6. A site only needs the ones it has installed, but a site with several calendar integrations has a list to work through rather than a single button to press.

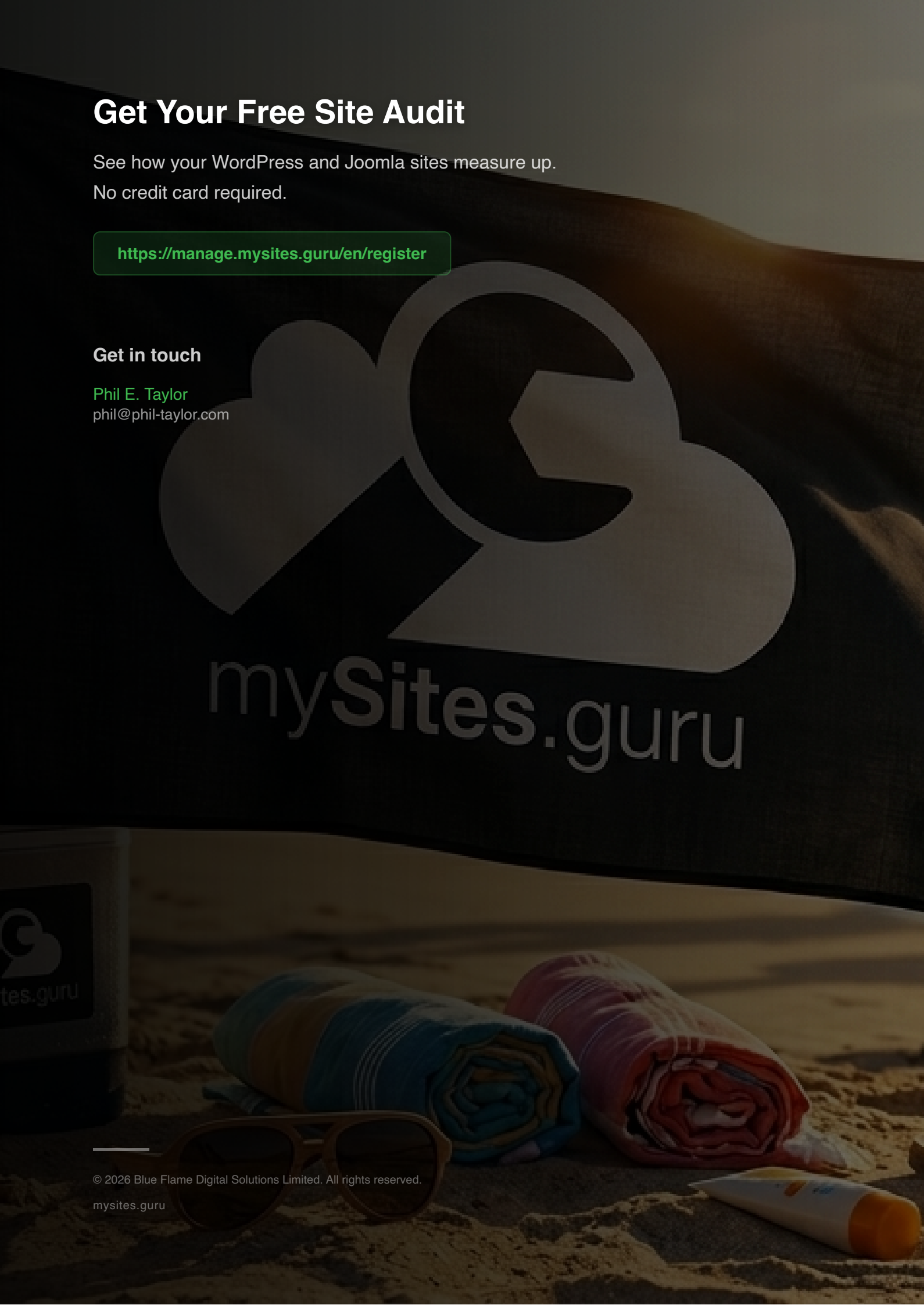
Written and edited by a human, with AI assistance. Our approach to AI

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