CVE-2026-97287

Routing around a working whitelist in Event Tickets

Intrudify's autonomous pentesting engine discovered a SQL injection vulnerability in **Event Tickets**, affecting all versions up to and including **5.29.5**. The plugin validates sort direction against an ASC and DESC whitelist, and that check works. Sending `orderby` as an array carries the direction through a different code path that never reaches the check, and straight into the `ORDER BY` clause.

DISCOVERED BY
Intrudify autonomous engine

VALIDATED & REPORTED BY
Tudor Lasuschevici

DISCLOSURE
30 September 2026

SEVERITY	VULNERABILITY CLASS
High · CVSS 8.5	SQL injection, CWE-89
AFFECTED	FIXED IN
Event Tickets ≤ 5.29.5	5.29.5.1

We use cookies

We use necessary cookies to run this site, and analytics cookies only if you accept. Change your choice anytime from the footer. Privacy Policy

Reject all Accept all

Tickets Commerce enabled, at least one

Summary

Event Tickets sells tickets and collects RSVPs for WordPress events. Intrudify's autonomous testing engine found that the Tickets Commerce Orders report takes its sort parameter from the request without validation, and that when that parameter arrives as an array, the sort direction is read from the array value and concatenated into the SQL.

The injected expression is evaluated by MySQL against the whole database, so a Contributor, the lowest role that can author a post, can read any table.

Technical detail

The value arrives unvalidated

In `src/Tickets/Commerce/Admin_Tables/Orders.php`:

```
$orderby = tribe_get_request_var( 'orderby' );        // line 157
...
if ( ! empty( $orderby ) ) {
    $arguments['orderby'] = $orderby;                 // line 211, no validation
}
```

The direction is taken from the array value

In `Order_Repository.php` the repository walks the parameter and decides which

We use cookies

We use necessary cookies to run this site, and analytics cookies only if you accept. Change your choice anytime from the footer.
Privacy Policy

Intrudify Contact Book a Demo

```
foreach ( $check_orderby as $key => $va
    $order_by = is_numeric( $key ) ? $
    ...
    $order    = is_numeric( $key ) ? $default_order : $value;
```

Sending `orderby[purchaser_full_name]=...` makes the key a string, so `$order` becomes the attacker-supplied array value. That value is passed on to the shared query filter.

Why the whitelist does not apply

This is the interesting part. The codebase does validate sort direction:

```
// common/src/Tribe/Repository.php:756
if ( ! in_array( $order, [ 'ASC', 'DESC' ], true ) ) {
    return $this;
}
```

That check is correct, strict, and effective. It simply lives in `order()`, which is reached only by the scalar `order` parameter. The array form carries its direction inside `orderby`, so it travels a path that never calls `order()` and is never checked. The defence exists and the attacker walks around it rather than through it.

The sink

In `common/src/Tribe/Repository/Query_Filters.php`:

```
$buffer[] = sprintf( '%s %s', $orderby, $order );
```

We use cookies

We use necessary cookies to run this site, and analytics cookies only if you accept. Change your choice anytime from the footer.
Privacy Policy

Intrudify Contact Book a Demo

WordPress adds backslashes to request values, which usually frustrates injection by breaking out of string literals. Here ds in an unquoted SQL context, so there is no string literal to escape from, and the working payload contains no quote characters at all. The protection is irrelevant rather than bypassed.

Verification

We confirmed this on a clean installation of WordPress 7.1, PHP 8.3, MariaDB 11 and Event Tickets 5.29.5 from the official wordpress.org package, with no other plugin present, using a stock Contributor account created through Users, Add New. That account's admin menu contains only Dashboard, Posts, Comments, Profile and Tools.

Response times against the same page in the same session, changing only the sort parameter:

orderby value	Time	Meaning
ASC	0.082 s	baseline
ASC,(SELECT SLEEP(2))	6.082 s	expression evaluated
ASC,(SELECT IF(1=1,SLEEP(2),1))	6.088 s	true branch
ASC,(SELECT IF(1=2,SLEEP(2),1))	0.079 s	false branch

The last two form a boolean oracle: true sleeps, false does not. The delay is a multiple of the number of rows the report lists, because MySQL evaluates the `ORDER BY` expression once per row, which is why three orders produce roughly six seconds from a two-second sleep.

We use cookies

We use necessary cookies to run this site, and analytics cookies only if you accept. Change your choice anytime from the footer.
Privacy Policy

Intrudify Contact Book a Demo

also captured the reached statement from the MariaDB general log, confirming the injection arrives in the query rather than being inferred from timing alone.

One note for anyone reproducing it: if the event has zero orders the page still returns 200 and the SQL still reaches the database, but MySQL never evaluates an `ORDER BY` expression over an empty result set, so nothing sleeps and the bug appears absent. The event needs at least one order.

Impact

Contributor is the lowest role that can author a post, and it is a role sites routinely hand to outside writers and guest event organisers. It grants no access to Users, Plugins, Settings or the Tickets screens.

With this vulnerability that account reads administrator password hashes and every user email address, along with every Tickets Commerce order record, which on this plugin means purchaser names, email addresses and payment metadata. The exposure is the whole database, not only the plugin's own tables.

The same sink is reachable through several sibling keys handled by the same switch, including `orderby[purchaser_email]` and `orderby[total_value]`, so fixing the single parameter we reported would not close it.

Remediation

Update Event Tickets to **5.29.5.1** or later.

For maintainers, the direction taken from the array form of `orderby` needs the same `ASC` and `DESC` validation the scalar form already receives, applied where

We use cookies

We use necessary cookies to run this site, and analytics cookies only if you accept. Change your choice anytime from the footer.
Privacy Policy

Intrudify Contact Book a Demo

The wider lesson

Nothing here is a missing check. The ASC and DESC whitelist is present, strict and correctly written, and a reviewer who finds it can reasonably conclude that sort direction is handled. The vulnerability is that a second path into the same sink does not pass through it.

The mechanism that creates the second path is worth recognising on its own: a parameter that accepts both a scalar and an array, with different code interpreting each shape. PHP makes this easy to do accidentally, because whether a request parameter arrives as a string or an array is entirely the caller's choice. Wherever a function branches on `is_numeric($key)` or `is_array($value)` to decide what a value means, the attacker, not the developer, picks which branch runs.

The generalisable check: find the sink first, then enumerate every path that reaches it, and confirm the validation sits on the sink rather than on one of the paths. Auditing from the defence outward, which is the natural direction for a human reading code, systematically misses the routes that bypass it.

Disclosure timeline

2026-09-15	Vulnerability identified and full chain validated by Intrudify, reported via Patchstack
2026-09-30	Public disclosure · CVE-2026-97287 assigned

We use cookies

We use necessary cookies to run this site, and analytics cookies only if you accept. Change your choice anytime from the footer.

Privacy Policy

plugin, versions 5.29.5 and earlier. It was discovered autonomously by the

Intrudify AI penetration testing engine. A Contributor can send the orderby parameter as an array, which bypasses validation past the ASC/DESC whitelist and concatenates it into the ORDER BY clause of the Tickets Commerce Orders report unescaped.

What can an attacker read with CVE-2026-97287?

The injected expression is evaluated by MySQL against the whole database, so any table is readable. We recovered the administrator username and the beginning of the administrator password hash from wp_users using a time-based boolean oracle, from a stock Contributor session.

How do I fix CVE-2026-97287?

Update Event Tickets to version 5.29.5.1 or later. The underlying fix is to validate the sort direction on the array form of orderby against the same ASC and DESC whitelist the scalar form already passes through, and to whitelist the column name rather than concatenating it.

References

CVE.ORG	CVE-2026-97287 record
NVD	National Vulnerability Database entry
PATCHSTACK	Patchstack advisory & mitigation rule
WORDFENCE	Wordfence Intelligence entry

We use cookies

We use necessary cookies to run this site, and analytics cookies only if you accept. Change your choice anytime from the footer.
Privacy Policy

Intrudify Contact Book a Demo

The two zeroes that compared equal in JetFormBuilder CVE-2026-107431

The heading level that never had to be a number in Kadence Blocks CVE-2026-105890

All discovered CVEs

We use cookies

We use necessary cookies to run this site, and analytics cookies only if you accept. Change your choice anytime from the footer.

Privacy Policy

PRODUCT

Platform

Services

Compliance

FAQs

Book a demo

COMPANY

Blog

Research Papers

Discovered CVEs

Customer Success Stories

Case Studies

Security

Contact

LEGAL

Privacy Policy

Terms of Service

Acceptable Use

Security Policy

HTML Sitemap

Cookie Preferences

CONNECT

Contact us

LinkedIn

GitHub

We use cookies

We use necessary cookies to run this site, and analytics cookies only if you accept. Change your choice anytime from the footer.
Privacy Policy