mySites.guru

EasyStore 3.0.1 Fixes Seven Security Flaws mySites.guru Found in 3.0.0 on Release Day

Before EasyStore 3.0.1, any visitor could pull a Joomla shop customer's home address and phone number from their email. mySites.guru found it and six more.

Phil E. Taylor | 23 September 2026

EasyStore is JoomShaper's ecommerce extension for Joomla: products, cart, checkout, orders and coupons. JoomShaper released EasyStore 3.0.0 on 10 September 2026, and within hours of it going out we had found seven security flaws in it during a code audit for mySites.guru customers. We reported them privately that day. EasyStore 3.0.1, released on 23 September, fixes all seven.

The one that matters most to a shop owner needs no login. EasyStore's guest checkout could be asked for any guest customer's saved shipping address by email address, and it answered: name, street address, city, postcode, country and phone number, to anyone.

TL;DR

- Update EasyStore to **3.0.1** now. Every version below it is affected, Free and Pro: we reported the flaws against 3.0.0 and the same code is in 2.0.1, so older 2.x shops are exposed too
- The worst needs **no login at all**: the guest checkout lookup returned a guest customer's full shipping address and phone number to any visitor who supplied their email address
- Five are in the administrator side: two SQL injections, no CSRF protection across the admin API, a configuration update that rewrote the site's mail sender with no token check, and an edit permission check that always returned yes
- The seventh affects logged-in customers, whose reviews a hostile page could post because the CSRF check was commented out
- JoomShaper handled this one well, sending us a build to verify before release and shipping 3.0.1 with a Security section listing seven reserved CVE IDs
- mySites.guru flags every connected site on an affected version, so you do not have to check each shop by hand

The seven flaws, and who can reach them

Whether a flaw needs a login decides how urgent it is, so here they are grouped that way, worst first.

#	Flaw	Who can exploit it	What it exposes
1	Guest checkout customer lookup (IDOR)	Anyone, no login	A guest customer's name, address and phone number
2	SQL injection in media image deletion	An administrator session	The database
3	SQL injection in coupon bulk update	An administrator session	The database
4	No CSRF check on the admin API	A logged-in admin who opens a hostile page	Product, order, customer and settings changes
5	Configuration update with no CSRF or access check	A logged-in admin who opens a hostile page	The site's mail sender name and address
6	`allowEdit()` always returns true	Any administrator	Edits Joomla's permissions should block
7	CSRF check commented out on reviews	A logged-in customer who opens a hostile page	Reviews posted in their name

The CVE records had not been published when we wrote this, so the order above follows our own provisional CVSS 4.0 scores: 8.7 High for the customer lookup, 8.6 High for each SQL injection, 6.9 Medium for the admin API CSRF and 5.1 Medium for the other three. The cards under Disclosure and severity show each vector. We will switch to the Joomla CNA's scores when they appear.

1. Any visitor could look up a customer's address by email

EasyStore's checkout has a helper that fills in the shipping form for a returning guest. When a guest types their email address, the browser sends it to `task=checkout.searchGuestUser` and gets the saved address back.

The controller took the email from the request, looked up the matching row in the guest customers table and returned its stored shipping address as JSON. There was no login check, no session check and no token, and nothing tied the request to the person who owned the address. Anyone could send the same request, from anywhere, with any email address.

So a customer's name, street address, city, postcode, country and phone number were one request away for anybody who knew or guessed their email. Email addresses are not secrets: they leak in breaches, sit on business cards and can be bought in bulk. An attacker with a list could test every address on it against a shop and keep the ones that returned a home address, which is also a reliable way to learn who shops there. We confirmed this live on our own test install.

In 3.0.1 the endpoint returns nothing at all and is marked as deprecated, with a code comment giving the personal data exposure as the reason. That is the right fix: the feature cannot be made safe without proving who is asking, and proving that is what logging in is for.

> **A lookup like this leaves no trace**
>
> Reading customer data writes nothing: no file changes, no new admin account, nothing a file scan would catch. If a shop with real guest customers ran EasyStore below 3.0.1, treat guest shipping details as potentially read, and check with whoever handles data protection for the business whether it has to be reported.

2 and 3. SQL injection in media deletion and coupon bulk update

Two admin endpoints built a SQL `IN()` list by gluing request values straight into the query. Media image deletion took an `ids` string, split it on commas and put the pieces into `WHERE id IN (...)` unchanged. Coupon bulk update did the same with a `cid[]` array.

Both need an administrator session. That sounds like a high bar, but administrator accounts are the ones that get phished, reused across sites and shared with contractors, and a SQL injection turns “can manage the shop” into “can read or change anything in the database”, including tables that have nothing to do with EasyStore. In 3.0.1 both paths convert every id to an integer and pass them through Joomla’s parameterised `whereIn()`, which is the correct, complete fix.

4 and 5. Admin changes a hostile page could trigger

Cross-site request forgery (CSRF) is the attack where a page on another site makes the victim’s browser send a request to yours without them knowing. The browser attaches the victim’s session cookie, so the request arrives logged in. Joomla’s defence is a form token that another site cannot know, and every state-changing request is supposed to check it.

EasyStore’s admin API controller did not check the token globally. Only its `products()` method did. Every other admin AJAX endpoint (media, coupons, customers, orders, tags, brands, categories, reviews, settings and collections) accepted state-changing requests without one. The configuration endpoint was a separate case of the same problem: it wrote the site’s sender name and email address into Joomla’s `configuration.php` with no token check and no access check.

This is why “needs an administrator” undersells these two. The attacker does not need an admin account. They need an administrator who is logged in to open a link, which is an easier thing to arrange. A changed mail sender tends to go unnoticed until password reset emails start behaving strangely.

In 3.0.1 the admin API checks the token for every POST, PUT, PATCH and DELETE request, and the configuration update now requires the right request method, admin

permission and a valid token.

6. A permission check that always said yes

Joomla lets a site owner restrict who can edit what, down to individual records. Controllers ask for that decision through `allowEdit()`. EasyStore's admin API overrode it like this:

```
protected function allowEdit($data = [], $key = 'id')
{
    return true;
}
```

So every edit routed through that controller skipped Joomla's asset permissions entirely. A shop manager the owner had restricted could edit anything the API could reach. In 3.0.1 the method asks EasyStore's access control class instead.

7. Reviews posted in a customer's name

The storefront review endpoint already had the right CSRF check written, and it was commented out:

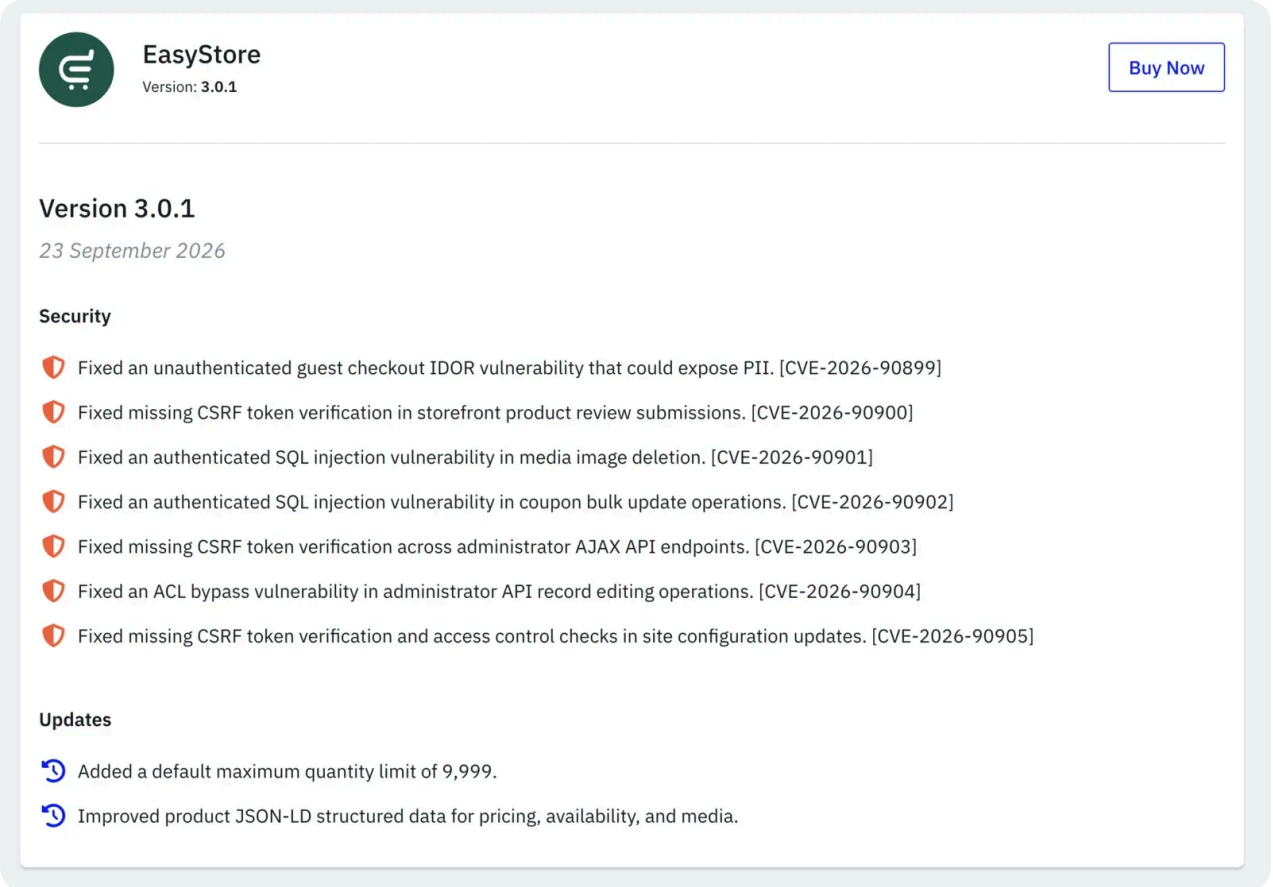
```
// Note: Uncomment CSRF check if frontend explicitly attaches standard Joo
// if (!\Joomla\CMS\Session\Session::checkToken('request')) {
//     $this->sendResponse(['status' => 'error', 'message' => Text::_('JIN
//     return;
// }
```

A hostile page could post reviews under any logged-in customer who visited it. It is the least serious of the seven, but fake reviews under real customer names are a reputational problem for a shop, and the fix was already sitting in the file. 3.0.1 enables the check and restricts the request method.

What JoomShaper got right this time

In July we reported three flaws in EasyStore 2.0.1. JoomShaper fixed them quickly, but shipped 2.0.2 with the fixes worded as routine changelog lines, with no security wording at all. This release was handled differently.

JoomShaper sent us the fixed build, Free and Pro, and asked us to confirm it before releasing. We did, against the code, and all seven were closed. Then 3.0.1 went out with a separate Security section that names each flaw by type and cites a CVE ID for each one:



A shop owner reading that knows it is a security release. The word “unauthenticated” is right there on the first line. Compare it with July, when the only hint that 2.0.2 closed a database-wide SQL injection was a line about “strict allowlist sanitization for product list sorting options”.

Two gaps remain. The changelog credits no one for finding the flaws, and the pairing of CVE IDs to fixes shown above is JoomShaper's own. The CVE records are the authority on that, and vendor changelogs have transposed IDs before, so we are not repeating the mapping as fact until the records publish.

Is 3.0.1 the end of it?

For the seven flaws in this post, yes: every one is fixed in 3.0.1's code. Reading 3.0.1 to confirm those fixes, we also found further issues that this release does not address. We are not publishing any detail about them.

That should not stop anyone updating. 3.0.1 closes everything described above, including the one any visitor could exploit, and staying on 3.0.0 or 2.x leaves all seven open. When there is more to say, we will say it here.

How do you update EasyStore safely?

1. **Take a backup first.** If you use mySites.guru, take a snapshot or run a full backup before touching a live shop.
2. **Update to 3.0.1.** On one site, use Joomla's System, Update, Extensions screen. Across several, use the mySites.guru mass updater to push it to every shop at once.
3. **Confirm the version.** Check the site's extension list shows EasyStore 3.0.1 or later.
4. **Check the mail settings.** In Joomla's Global Configuration, confirm the From Email and From Name are what you set, since the configuration flaw could change them.
5. **Review your administrator accounts.** Several of these flaws were reachable through an administrator's session, so look for accounts and changes you do not recognise.

Find administrator accounts you never created

mySites.guru checks every connected site for this automatically and flags it the moment it appears. It runs as part of the full audit on every connected site.

Check your site for free →

How do I find every EasyStore shop I manage?

On release day, every EasyStore install in the mySites.guru database with a readable version number was on an affected version. Well over half were already on 3.0.0, less than two weeks after it came out, which says something good about how quickly EasyStore shops update. It also means the flaws reached most shops almost as soon as they shipped.

The first question after a release like this is which of your sites run the thing. mySites.guru keeps a live inventory of the extensions, plugins and templates on each connected Joomla and WordPress site. Search for EasyStore once and you see each shop running it and the version each one is on.

We added the affected range, every version below 3.0.1, to the mySites.guru vulnerability database today, so every connected site still on a vulnerable EasyStore is flagged on its dashboard without anyone searching. The same database lists the Joomla extension vulnerabilities we track, with the affected versions for each.

What else mySites.guru checks on a Joomla shop

EasyStore is one extension. A typical Joomla shop runs dozens, and each has its own release notes, its own version numbering and its own idea of what counts as a security release. No single check covers that. It takes several running together:

- Vulnerable extension detection compares installed extensions against the known-vulnerable ranges and flags the site as soon as one matches. That is how today's EasyStore rule reaches every connected shop at once.
- Rogue administrator detection lists super users you did not create, which is where admin-side flaws tend to leave their mark.
- File scanning checks every file against a pattern library of roughly 1,500 malware signatures and looks for files that can accept uploads.
- The mass updater pushes the fixed version to every affected site from one screen once you know which ones they are.

All of it runs unattended across every connected site, and all of it is part of the subscription. Doing the same by hand means logging into each Joomla admin, reading the extensions list and comparing it against changelogs, and doing it again the next time a vendor ships.

If a shop has already been hit, fix.mySites.guru cleans it, audits it for backdoors and hands it back secure for a single fixed fee, usually the same day. Non-subscribers get a free month with it.

Start with a free audit on one site to see what it finds, or see the plans and connect every site you manage.

Disclosure and severity

We found all seven flaws reading EasyStore 3.0.0's code and confirmed the unauthenticated customer lookup live on our own test install. They were reported privately to JoomShaper on 10 September 2026, with the Joomla Security Strike Team copied, and nothing was published until the fix shipped.

The weakness classes are an insecure direct object reference (CWE-639) for the customer lookup, cross-site request forgery (CWE-352) for the review, admin API and configuration flaws, SQL injection (CWE-89) for the media and coupon endpoints, and incorrect authorization (CWE-863) for `allowEdit()`.

We scored each finding under CVSS 4.0 ourselves while the CVE records are unpublished. These are provisional: when the Joomla CNA publishes its scores we will switch to them, and say so here if they differ. The CVE ID on each card follows JoomShaper's 3.0.1 changelog and will be checked against the records when they publish. Worst first:

8.7
CVSS 4.0

CVE-2026-90899 Unauthenticated guest checkout IDOR exposing customer PII

HIGH

mySites.guru assessment, 23 September 2026. Provisional: the CVE records were not yet published, and the Joomla CNA may score this differently.

Guest checkout customer lookup. Any visitor who supplies a guest customer's email address gets back their name, street address, city, postcode, country and phone number.

`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N`

No login needed · Exploitable over the internet · Customer personal data

▼ What does this mean?

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

How it is reached

`AV:N` Network: Reachable across the internet
`AC:L` Low: Nothing to work around, it just works
`AT:N` None: Works against any affected install
`PR:N` None: No account needed
`UI:N` None: Nobody has to be tricked into anything

What it does to the site

`VC:H` High: Everything the site holds can be read
`VI:N` None: Nothing can be altered
`VA:N` None: The site stays up

What it does beyond the site

`SC:N` None: Other systems keep their data
`SI:N` None: Other systems keep their integrity

SA:N None: Other systems stay up

8.6
CVSS 4.0

CVE-2026-90901 Authenticated SQL injection in media image deletion

HIGH

mySites.guru assessment, 23 September 2026. Provisional: the CVE records were not yet published, and the Joomla CNA may score this differently.

SQL injection in media image deletion. An administrator session can read or change anything in the site database.

`CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N`

▼ What does this mean?

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

How it is reached

AV:N Network: Reachable across the internet
AC:L Low: Nothing to work around, it just works
AT:N None: Works against any affected install
PR:H High: Needs an account with elevated rights
UI:N None: Nobody has to be tricked into anything

What it does to the site

VC:H High: Everything the site holds can be read
VI:H High: Data and files can be altered at will
VA:H High: The site can be taken down

What it does beyond the site

SC:N None: Other systems keep their data
SI:N None: Other systems keep their integrity
SA:N None: Other systems stay up

8.6
CVSS 4.0

CVE-2026-90902 Authenticated SQL injection in coupon bulk update

HIGH

mySites.guru assessment, 23 September 2026. Provisional: the CVE records were not yet published, and the Joomla CNA may score this differently.

SQL injection in coupon bulk update. The same flaw as the media endpoint, reached through the coupon ids.

`CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N`

▼ What does this mean?

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

How it is reached

`AV:N` Network: Reachable across the internet
`AC:L` Low: Nothing to work around, it just works
`AT:N` None: Works against any affected install
`PR:H` High: Needs an account with elevated rights
`UI:N` None: Nobody has to be tricked into anything

What it does to the site

`VC:H` High: Everything the site holds can be read
`VI:H` High: Data and files can be altered at will
`VA:H` High: The site can be taken down

What it does beyond the site

`SC:N` None: Other systems keep their data
`SI:N` None: Other systems keep their integrity
`SA:N` None: Other systems stay up

6.9
CVSS 4.0

CVE-2026-90903 Missing CSRF token verification across the administrator AJAX API

MEDIUM

mySites.guru assessment, 23 September 2026. Provisional: the CVE records were not yet published, and the Joomla CNA may score this differently.

No CSRF check across the admin API. A logged-in administrator who opens a hostile page can be made to change products, orders, customers and settings.

`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N`

Needs an admin to open a link

▼ What does this mean?

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

How it is reached

`AV:N` Network: Reachable across the internet
`AC:L` Low: Nothing to work around, it just works
`AT:N` None: Works against any affected install
`PR:N` None: No account needed
`UI:A` Active: Someone has to be talked through a few steps

What it does to the site

`VC:N` None: Nothing can be read
`VI:H` High: Data and files can be altered at will
`VA:N` None: The site stays up

What it does beyond the site

`SC:N` None: Other systems keep their data
`SI:N` None: Other systems keep their integrity
`SA:N` None: Other systems stay up

5.1
CVSS 4.0

CVE-2026-90905 Missing CSRF and access control checks in site configuration updates

MEDIUM

mySites.guru assessment, 23 September 2026. Provisional: the CVE records were not yet published, and the Joomla CNA may score this differently.

Configuration update with no CSRF or access check. A hostile page can rewrite the site's mail sender name and address in configuration.php.

`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N`

Needs an admin to open a link

▼ What does this mean?

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

How it is reached

`AV:N` Network: Reachable across the internet
`AC:L` Low: Nothing to work around, it just works
`AT:N` None: Works against any affected install
`PR:N` None: No account needed
`UI:A` Active: Someone has to be talked through a few steps

What it does to the site

`VC:N` None: Nothing can be read
`VI:L` Low: Some data can be altered
`VA:N` None: The site stays up

What it does beyond the site

`SC:N` None: Other systems keep their data
`SI:N` None: Other systems keep their integrity
`SA:N` None: Other systems stay up

5.1
CVSS 4.0

CVE-2026-90904 ACL bypass in administrator API record editing

MEDIUM

mySites.guru assessment, 23 September 2026. Provisional: the CVE records were not yet published, and the Joomla CNA may score this differently.

allowEdit() always returns true. Any administrator can edit records that Joomla's asset permissions should stop them editing.

`CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N`

▼ What does this mean?

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

How it is reached

`AV:N` Network: Reachable across the internet
`AC:L` Low: Nothing to work around, it just works
`AT:N` None: Works against any affected install
`PR:H` High: Needs an account with elevated rights

UI:N None: Nobody has to be tricked into anything

What it does to the site

VC:N None: Nothing can be read
VI:L Low: Some data can be altered
VA:N None: The site stays up

What it does beyond the site

SC:N None: Other systems keep their data
SI:N None: Other systems keep their integrity
SA:N None: Other systems stay up

5.1
CVSS 4.0

CVE-2026-90900 Missing CSRF token verification on storefront product reviews

MEDIUM

mySites.guru assessment, 23 September 2026. Provisional: the CVE records were not yet published, and the Joomla CNA may score this differently.

CSRF on storefront reviews. A hostile page can post reviews in the name of any logged-in customer who visits it.

`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N`

Needs a customer to open a link

▼ What does this mean?

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

How it is reached

AV:N Network: Reachable across the internet
AC:L Low: Nothing to work around, it just works
AT:N None: Works against any affected install
PR:N None: No account needed
UI:A Active: Someone has to be talked through a few steps

What it does to the site

VC:N None: Nothing can be read
VI:L Low: Some data can be altered
VA:N None: The site stays up

What it does beyond the site

```
SC:N  None: Other systems keep their data
SI:N  None: Other systems keep their integrity
SA:N  None: Other systems stay up
```

Field	Detail
Extension	EasyStore for Joomla (`com_easystore`), Free and Pro
Vendor	JoomShaper (joomshaper.com)
Affected versions	Everything below 3.0.1 (reported against 3.0.0, also present in 2.0.1)
Fixed in	EasyStore 3.0.1, released 23 September 2026
CVE	CVE-2026-90899, CVE-2026-90900, CVE-2026-90901, CVE-2026-90902, CVE-2026-90903, CVE-2026-90904, CVE-2026-90905, reserved through the Joomla CNA, records not yet published
CVSS 4.0	Our provisional scores: 8.7 High (customer lookup), 8.6 High (each SQL injection), 6.9 Medium (admin API CSRF), 5.1 Medium (configuration CSRF, allowEdit, review CSRF). No Joomla CNA scores yet
Finder	Phil Taylor, mySites.guru
Reported	10 September 2026, to JoomShaper, with the Joomla Security Strike Team copied
Acknowledged	10 September 2026
Fix verified	22 September 2026, against a pre-release build JoomShaper sent us
Vendor credit	None in the 3.0.1 changelog

Timeline

2026-09-10 — **JoomShaper releases EasyStore 3.0.0**

A major release of the Joomla ecommerce extension, Free and Pro.

2026-09-10 **mySites.guru reports seven flaws the same day**
Sent privately to JoomShaper, with the Joomla Security Strike Team copied. No public detail.

2026-09-10 **JoomShaper acknowledges the report**
Support thanks us and passes the findings to the developers to verify.

2026-09-22 **JoomShaper sends a fixed build for checking**
Free and Pro, with a request to confirm before release.

2026-09-22 **mySites.guru confirms all seven are fixed**
Checked against the code of the build JoomShaper sent.

2026-09-23 **EasyStore 3.0.1 ships with a Security section**
Seven fixes, each citing a reserved CVE ID. No reporter credit.

2026-09-23 **Affected sites flagged and this post published**
Every connected site below 3.0.1 is flagged in mySites.guru.

Further Reading

- Exposed customer invoices, order forgery and SQL injection in EasyStore - the three flaws we reported in EasyStore 2.0.1, fixed in 2.0.2.
- The Joomla extension security disclosure standard - the Joomla Security Strike Team's twenty rules for extension developers, including CVEs and reporter credit.
- Front-end AJAX endpoints are a CMS security blind spot - why an anonymous request can reach customer data.
- How to check your Joomla database security - what to review if a vulnerable extension was live.

- CWE-639: Insecure Direct Object Reference, CWE-352: Cross-Site Request Forgery and CWE-89: SQL Injection - the weakness classes behind these seven.
- EasyStore by JoomShaper - the vendor's product page, where 3.0.1 is available.

Frequently Asked Questions

What is the most serious EasyStore 3.0.0 flaw?

A guest checkout lookup that returned a customer's saved shipping address to anyone who asked. Send the endpoint an email address and it replied with that guest customer's name, street address, city, postcode, country and phone number. No login, no session and no token were needed, so anyone who could guess or buy a list of email addresses could check it against a shop's guest customers. EasyStore 3.0.1 removes it.

Which EasyStore versions are affected?

Everything below 3.0.1. We reported the flaws against 3.0.0, and all seven are also present in the 2.0.1 code, so older 2.x installs are affected too. The fix is EasyStore 3.0.1, released 23 September 2026, for both the Free and Pro editions.

Do the admin-side flaws matter if my administrators are trusted?

Yes, for two reasons. Two of the admin-side flaws are cross-site request forgery, which means the attacker never needs an admin account: they need an administrator who is logged in to open a page they control. And an administrator account that is phished, reused or shared with a contractor becomes a route to SQL injection and to edits Joomla's permissions should have blocked.

Are there CVEs for these flaws?

Seven CVE IDs are reserved through the Joomla CNA, CVE-2026-90899 to CVE-2026-90905, and JoomShaper cites them in the 3.0.1 changelog. The records had not been published when we wrote this, so there are no official CVSS scores yet. Our own provisional CVSS 4.0 scores run from 8.7 High for the customer lookup down to 5.1 Medium, and we will switch to the Joomla CNA's scores once the records appear.

Is EasyStore 3.0.1 completely secure?

3.0.1 fixes all seven flaws we reported, and we confirmed that in the code before release. Reading 3.0.1 we also found further issues that this release does not address. We are not publishing any detail about them. Update to 3.0.1 now regardless, because it closes everything described here.

How do I find every EasyStore shop I manage?

mySites.guru keeps a live inventory of every extension on every connected Joomla site and flags any site running an EasyStore version below 3.0.1 automatically. You search once, see

every shop and its version, and push the update to all of them from one screen.

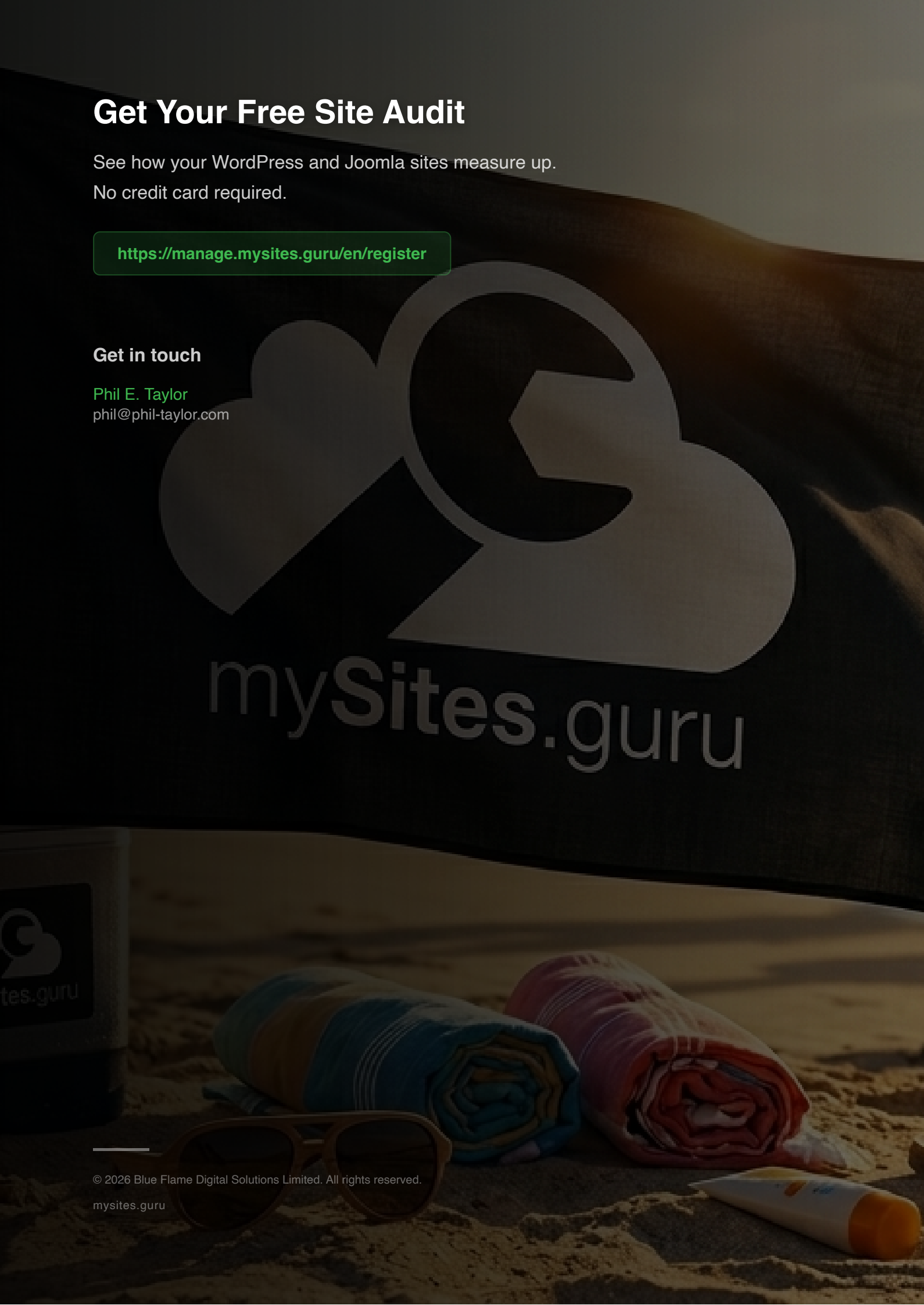
Written and edited by a human, with AI assistance. Our approach to AI

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