



Event Gallery 6.6.0 Fixes Forged Backend Changes and a Google Photos Token Leak

Event Gallery 6.6.0 fixes CVE-2026-102776, a backend CSRF, CVE-2026-102777, a Google Photos token leak, and a Low XSS. Every Joomla site below 6.6.0 needs it.

Phil E. Taylor | 4 October 2026

Sven Bluege released [Event Gallery 6.6.0](#) for Joomla on 4 October 2026, eight days after the [6.5.0 security release](#). It fixes three more vulnerabilities. Eight buttons in the backend lists could be triggered from another website, the Google Photos picker could be made to send its access token to any address, and the page a shared image link opens could run script or redirect the visitor.

All three are still present in 6.5.0. A site you updated last week is affected again, and so is every site still below it.

What to do now

Update Event Gallery to 6.6.0 on every Joomla site that runs it, Core and Extended alike, including sites already on 6.5.0. 6.6.0 needs Joomla 5.4 or later, or Joomla 6, and PHP 8.2, so a site still on Joomla 3 or 4 has to upgrade Joomla first. If you override the backend layout `tmpl/files/default.php` in your template, copy the star and table-icon buttons from the new file, or they stop with a token warning.

5.1

CVSS 4.0

CVE-2026-102776: forged changes from the backend lists

MEDIUM

Our assessment (CVE record not yet published); matches the vendor's 5.1

A page on another website could change payment and shipping defaults, image type sets, order statuses, watermarks and image flags through a logged-in administrator. Nothing can be deleted or read.

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

Logged-in admin opens a page

Every version below 6.6.0

▼ 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-2026-102777: Google Photos access token sent elsewhere

MEDIUM

Our assessment (CVE record not yet published); matches the vendor's 5.1

The server could be made to send the Google Photos access token to any address, or to fetch addresses inside its own network. Only sites with a Google Photos account set up.

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

Logged-in admin opens a page

5.4.0 to below 6.6.0

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

What it does beyond the site

SC:L Low: Some data on other systems can be read
SI:N None: Other systems keep their integrity
SA:N None: Other systems stay up

TL;DR

- Event Gallery 6.6.0 fixes CVE-2026-102776, CVE-2026-102777 and a third issue, EGSA-2026-08, that has no CVE
- CVE-2026-102776: eight backend list buttons did not check Joomla's form token, so a prepared page could change shop and gallery settings through a logged-in administrator. It affects every version below 6.6.0
- CVE-2026-102777: the Google Photos thumbnail proxy fetched whatever address it was given, with the account's access token attached and no form token. Sites with a Google Photos account, from 5.4.0
- EGSA-2026-08 (Low): with Share article links switched on, a shared image link could run script or redirect the visitor. From 3.11.6, and the option is off by default
- 6.5.0 is affected by all three. About two in five Event Gallery installs we monitor moved to 6.5.0 in the last eight days, and all of them need 6.6.0 now
- mySites.guru flags every connected Joomla site running Event Gallery below 6.6.0

Forged changes from the backend lists (CVE-2026-102776)

Joomla protects every form with a token, a value the server checks so it can tell a request the user made from one another website made on their behalf. Eight buttons in Event Gallery's backend lists skipped that check. According to the vendor's notes, they set:

- the default payment method and the default shipping method
- the default of the image type sets, order statuses and watermarks
- whether an event is In shop
- the main image of an event, and whether an image is shown only as the main image
- the sort order of an event's images

Each was a plain link. If an administrator who was logged in to the backend opened a page that requested one of those links in the background, the change went through with their session. On a photo shop, that is enough to switch the default payment or shipping method, swap the watermark, take an event out of the shop or reorder and hide its images.

The vendor sets out the limits: nothing could be deleted or read this way, and orders were not affected. It is a nuisance and an integrity problem, not a takeover. The same class of bug was behind three of the five CVEs fixed in 6.5.0, and we score this one the same 5.1 the Joomla CNA gave the 6.5.0 upload and clean-up CSRFs.

6.6.0 makes all eight require the token. The star and the table icon in the image list now submit the list form the way the publish icon next to them does, instead of following a link. That is the one change a site owner can trip over: a template override of the backend `tmpl/files/default.php` still holds the old links, and they will stop with Joomla's invalid token warning until you copy the two buttons from the new file.

The Google Photos token leak (CVE-2026-102777)

Event Gallery can pull images from a Google Photos account. On the upload page, the picker shows thumbnails, and Event Gallery fetches those thumbnails through your own server, sending the Google Photos access token with each request so Google will serve them.

Before 6.6.0, the address to fetch came from the request and was not checked, and the request needed no form token. Put those together and a page on another website could make your server send the Google Photos access token to an address of the attacker's

choosing, or fetch addresses inside your own network, while an administrator was logged in to the backend. A backend user with permission to manage Event Gallery could do the same directly, without anyone being tricked.

The leaked token is a credential for the connected Google Photos account, and the internal fetches are a classic server-side request forgery: the web server can usually reach things the outside world cannot. Only sites with a Google Photos account set up in Event Gallery are affected, from 5.4.0 on. 6.6.0 fetches only addresses on Google's image hosts and requires the form token on the picker requests. The vendor also added a random state value to the Google Photos authorisation, checked against the session on the way back, as hardening without a known vulnerability.

If you did connect a Google Photos account and cannot rule out that an administrator opened something they should not have, disconnect and reconnect the account after updating, so that any token issued before the fix stops working. That step is our advice, not the vendor's.

The shared image link XSS and open redirect (EGSA-2026-08)

The third issue is rated Low by the vendor (2.3) and has no CVE. With the option Share article links switched on, the page a shared image link opens links back to the article the image was shared from. It took that article's address straight from the shared link and printed it as it came, and with the link type Image Page with Redirect it followed the address at once.

A crafted link could therefore run script in the page, in the session of whoever opened it, or send the visitor to another website. Only sites with Share article links on are affected, from 3.11.6, and the option is off unless someone switched it on. 6.6.0 follows only an address on your own site and escapes it. Until you can update, switch Share article links off in the Event Gallery options, on the Social tab.

Why sites on Event Gallery 6.5.0 need to update again

Eight days ago, 6.5.0 was the answer. Since then, about two in five of the Event Gallery installs connected to mySites.guru have moved to it. All of those sites is affected by [CVE-2026-102776](#), and those with a Google Photos account by [CVE-2026-102777](#) as well. On the morning 6.6.0 came out, only a handful of the installs we monitor had it, and 99% were below it.

The update itself is light. 6.6.0 has the same requirements as 6.5.0 (Joomla 5.4 or later, or Joomla 6, and PHP 8.2), so any site that took 6.5.0 can take 6.6.0 in a couple of minutes. The release also makes orders, payments and mails more reliable and prepares Event Gallery for Joomla 7, and its migration hints are worth a read before you update a shop. If your checkout uses a template override of `checkout/review.php`, it needs one new hidden field, and Stripe no longer offers SEPA Direct Debit, Sofort or Giropay.

The sites that cannot take it are the same ones that could not take 6.5.0. Of the affected sites we monitor, 64% run Joomla 5.4 or later, 29% are on Joomla 3 and 7% on Joomla 4. For the third on Joomla 3, there is no Event Gallery build with these fixes, and the real job is [getting off Joomla 3](#).

This time the release page did its job. 6.6.0 opens with a sentence saying it fixes three vulnerabilities, links to a Security Fixes section that sits above the features, and gives each fix an advisory id, a CVE where there is one, a severity, the versions affected and what to do before you can update. That is the format we asked for in [our 6.5.0 post](#), and it is what lets someone looking after dozens of sites decide in a minute that this one goes out today.

How mySites.guru flags Event Gallery below 6.6.0

mySites.guru records the exact version of each extension on each connected Joomla site twice a day. Our Joomla vulnerability database had an entry for Event Gallery below 6.6.0 on the day the release came out, so a connected site running an older component is flagged on its dashboard and in its audit, whether it runs Core or Extended. The [Event Gallery page of our vulnerability list](#) shows both Event Gallery rules, and the [vulnerable extension list](#) explains how the flags work across all the extensions we track.

The same audit checks the Joomla core version, which decides how much work each flagged site needs. A site on Joomla 5.4 or later can be updated in bulk from one dashboard. A site on Joomla 3 or 4 goes on the upgrade list.

Joomla CMS Version Must Be Up-to-date

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 →

What can I do before I can update Event Gallery?

Both CVEs need a logged-in backend user to open a page or link an attacker prepared, so the exposure is the set of accounts with backend access to Event Gallery and what those people browse while logged in.

- Switch Share article links off in the Event Gallery options (Social tab), which closes EGSA-2026-08
- If you no longer use the Google Photos integration, remove the account from Event Gallery
- Review who can manage Event Gallery in the backend and remove that permission where it is not needed
- Ask administrators to log out of the backend before browsing elsewhere
- Check the payment and shipping defaults, watermarks and In shop flags of your events if anything about the shop looks different, and run a full site audit

None of that replaces the update. If you look after more than a few Joomla sites, mySites.guru shows you which ones run Event Gallery below 6.6.0, and the Joomla version each one is on, from one dashboard.

Further Reading

- [Event Gallery Core 6.6.0 release page](#) - the vendor's notes, with the Security Fixes section first
- [Event Gallery downloads](#) - Core and Extended packages
- [OWASP Cross-Site Request Forgery Prevention Cheat Sheet](#) - why every state-changing request needs a form token
- [OWASP Server-Side Request Forgery Prevention Cheat Sheet](#) - the allow-list approach 6.6.0 takes for the Google Photos thumbnails
- [CWE-352: Cross-Site Request Forgery](#) and [CWE-918: Server-Side Request Forgery](#) - the two weakness classes behind the CVEs

Frequently Asked Questions

Is Event Gallery 6.6.0 a security release?

Yes. Sven Bluege released Event Gallery 6.6.0 on 4 October 2026 and labels it Security: Medium. It fixes three vulnerabilities: [CVE-2026-102776](#) (forged changes from the backend lists), [CVE-2026-102777](#) (the Google Photos picker could send its access token elsewhere) and EGSA-2026-08 (an XSS and open redirect on the shared image page, rated Low). Every version below 6.6.0 is affected by at least the first one.

I updated Event Gallery to 6.5.0 last week. Do I need to update again?

Yes. 6.5.0 closed five earlier issues, but all three fixed in 6.6.0 are still present in 6.5.0. Update every site to 6.6.0. It has the same requirements as 6.5.0: Joomla 5.4 or later, or Joomla 6, and PHP 8.2.

Is my site affected by the Google Photos token leak?

Only if Event Gallery runs 5.4.0 or later below 6.6.0 and a Google Photos account is set up in Event Gallery. Sites that never connected a Google Photos account are not affected by [CVE-2026-102777](#), but they are still affected by [CVE-2026-102776](#), which covers every version below 6.6.0.

Can these Event Gallery flaws be used to take over a Joomla site?

Not on their own. [CVE-2026-102776](#) changes shop and gallery settings and flags, and the vendor says nothing can be deleted or read through it. [CVE-2026-102777](#) leaks the Google Photos access token and lets the server be used to fetch addresses inside its own network, which is a credential and network exposure rather than code execution. Both need a logged-in backend user to open a page an attacker prepared.

Have CVE-2026-102776 and CVE-2026-102777 been published?

Not yet. Both ids are reserved by the Joomla CNA and named on the vendor's release page, but the CVE records had not been published when 6.6.0 came out, so there is no official CVSS score yet. The scores in this post are our own assessment and match the vendor's 5.1 for both.

How do I find every site that still runs Event Gallery below 6.6.0?

mySites.guru records the version of every extension on every connected Joomla site twice a day, and its Joomla vulnerability database flags Event Gallery below 6.6.0 from the day the

release came out. Every affected site shows the warning on its dashboard and in its audit.

AI MODIFIED

Written and edited by a human, with AI assistance. [Our approach to AI](#)

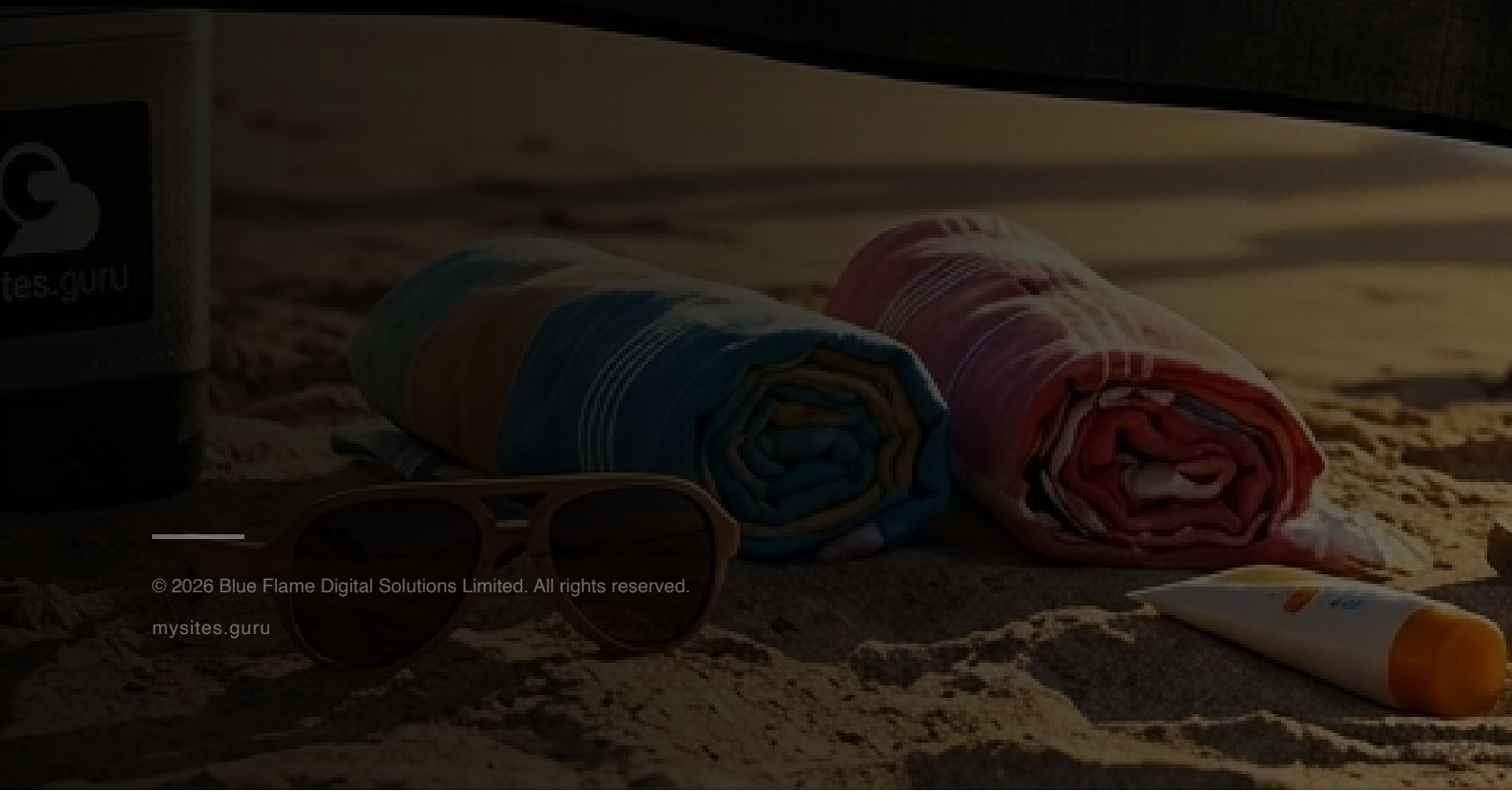
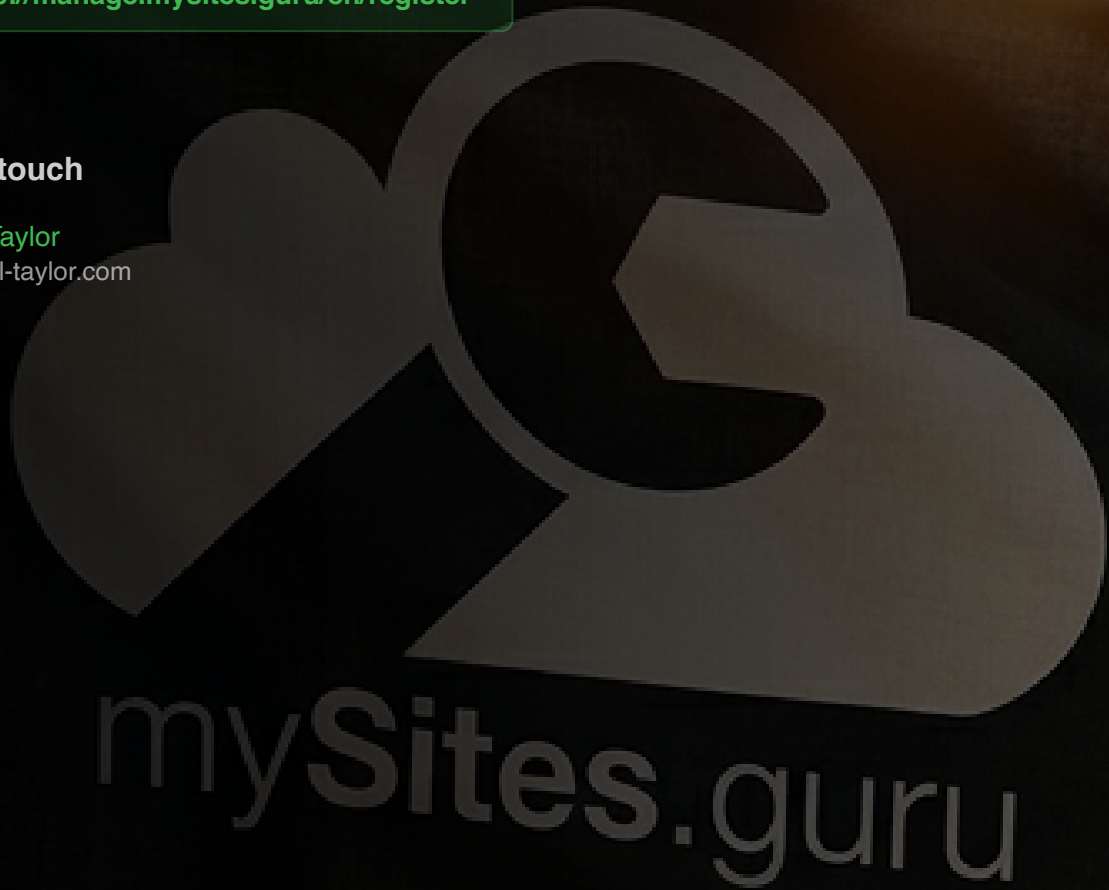
Get Your Free Site Audit

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



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

mysites.guru