



Ruth Cheesley

Implementing GitHub's private security issue reporting

FOSS Backstage
Berlin, 10-11 March 2025



@RCheesley



Ruth Cheesley (she/her)

**Mautic Project Lead &
Co-Founder, Women of Open
Source community**

ruth.cheesley@mautic.org

speaking.ruthcheesley.co.uk for slides, recording,
links and resources





Let's **secure open source** code, **together**.

Hunt for bounties and reap the rewards!

[Get started with GitHub](#)



How it works

Secure open source - simple



Disclose

Discover a new vulnerability, disclose it using our form, and reap the rewards!



Fix

Pick a vulnerability that takes your interest, fork its repo, and submit your fix.



Earn

Bounties are reviewed weekly, with cash, credits and prizes to be won.



Collaborate

Contribute to a bounty with other hunters and share the reward.

Disclose

Think you have found a vulnerability in open source?



Sign in with GitHub

At the click of a button, you can join our platform with your GitHub account.



Fill in our form

We have designed a disclosure form that allows you to help us investigate a vulnerability.



Earn your reward

After we have verified your disclosure, we will reward you for your effort.

✓ Quick Process ✓ Rewards every time ✓ Spread your name



Fix

Who doesn't want to get paid for fixing open source?



Pick a vulnerability

Select one from the bounty board and get fixing!



Submit your fix

Download the code, commit a patch and open a pull request. It's as simple as that.



Earn your reward

Every week we review the fixes and select the best ones.



Centralising the process of working on security issues.

We used this system to:

- Receive private security reports from researchers
- Centralise all communication between researcher, security team and marketing team on fixing and disclosure
- Pay micro bounties from their \$100 per project pot to researchers and developers





Hi rcheesley,

Thank you for being part of huntr: the most effective security community in the world. With your collaboration, we've achieved top CNA status, profoundly influencing both the open source ecosystem and the security landscape at large.

Thanks to our successes, huntr.dev has joined [Protect AI](https://protect.ai), a leading startup in AI/ML security and has become huntr.com

This acquisition brings expertise and resources to tackle the critical need for AI/ML security head-on with its unique challenges that span across source code, data, and models.

To address these challenges effectively and make a tangible impact on building a safer AI powered world, we will focus all of our efforts in this direction:

- Starting today, huntr.com will solely support vulnerabilities and remediations related to AI and ML libraries and frameworks.
- We will discontinue our active support of all non-AI/ML open-source projects from November 30th, 2023.

18th October, 2023: Our security reporting tool closes to non-AI/ML

Rather unexpected news!

- 6 weeks to find a new system for our security issue collaboration
- Needed to transfer all our publicised security issues too, as we wouldn't be able to make any edits after that date
- Opportunity to revisit what our security team - and our wider ecosystem - actually needed from our security reporting workflows







We had some frustrations with our existing processes, though!

- Couldn't easily collaborate on fixes directly in the code (e.g. with PRs) with the researchers
- Very minimal information provided in reports about the vulnerability
- Juggling 3 systems - Jira, Huntr and GitHub
- Multi-version fixes were a *real* pain to manage and release - lots of manual work!
- There was no central list of security advisories that had previously been released



The screenshot shows the GitHub interface for the `mautic/mautic` repository. The top navigation bar includes links for Product, Solutions, Open Source, and Pricing, along with a search bar and Sign in/Sign up buttons. The repository's main navigation bar shows Code, Issues (148), Pull requests (283), Discussions, Actions, Projects (1), Security (20), and Insights. A sidebar on the left contains links for Overview, Reporting, Policy, and Advisories (20). The main content area is titled "Security Advisories" and includes a description: "View known security vulnerabilities and report new vulnerabilities privately to maintainers." A green button labeled "Report a vulnerability" is highlighted with a red box. Below this, a list of ten security advisories is displayed, each with a title, a GitHub Security Advisory ID, a publication date, the reporter's name, and a severity level. The advisories include XSS vulnerabilities in tracking pixel functionality, htaccess file, installer, asset view, contacts view, and password reset page, as well as a broken cryptographic algorithm, secret data exfiltration, and a CSV injection vulnerability.

Advisory Title	Severity
XSS vulnerability in tracking pixel functionality	Critical severity
Improper regex in htaccess file	Moderate severity
XSS vulnerability in installer	High severity
Use of a Broken or Risky Cryptographic Algorithm	Low severity
XSS vulnerability on asset view	High severity
XSS vulnerability on contacts view	High severity
Stored XSS vulnerability on Bounce Management Callback	High severity
XSS vulnerability on password reset page	Moderate severity
Secret data exfiltration via symfony parameters	Moderate severity
CSV Injection vulnerability with exported contact lists	Moderate severity

Possible solution: GitHub Security Advisories?

A new feature: allowing the public to securely and privately report vulnerabilities with a repository directly, as a draft security advisory for the team to review.



Security Advisories

New draft security advisory

Privately discuss, fix, and publish information about security vulnerabilities in your repository's code.

 2 Triage

 2 Draft

 0 Published

 0 Closed

 **Remote denial of service in Go Package**

GHSA-xvhr-5836-ff96 opened 1 minute ago by security-researcher-1

Triage

 **Arbitrary code execution in Maven Package**

GHSA-fqhv-3x8m-cw5q opened 2 minutes ago by security-researcher-2

Triage

Critical severity

Creates a triage backlog for the team to review.

Allows reviewing and triaging, accepting or rejecting the report based on whether it meets the policies of the project. We could also generate our own advisories directly.





Open a draft security advisory

After the draft security advisory is open, you can privately discuss it with collaborators and create a temporary private fork where you can collaborate on a fix. If you've already fixed the vulnerability, just fill out the draft security advisory and then publish it.

Advisory Details

Title *

CVE identifier

Description *

Affected products

Severity

Weaknesses

Credits

Access and visibility

Once published, security advisories on public repositories are visible to everyone.

Once reviewed by GitHub, security advisories may be broadcast on the [GitHub Advisory Database](#). They may also trigger Dependabot alerts in users that depend on this repository.

Affected products

Ecosystem

Package name

Affected versions

Patched versions

+ Add another affected product

Go

e.g. example.js

e.g. < 1.2.3

e.g. 1.2.3

Cancel

Create draft security advisory

Users create a draft advisory to report issues.

- Comments in the advisory are never made public - only the content of the advisory itself





Collaborate on a patch in private

Use a temporary private fork of **octo-org/octorepo** to collaborate on a fix.

Start a temporary private fork



Accept vulnerability report

This potential security vulnerability was reported by someone external to your organization. Review carefully and accept to continue collaborating privately as a draft security advisory.

Accept and open as draft



Write

Preview

H B I @

Leave a comment

Attach files by dragging & dropping, selecting or pasting them.

M+

Close security advisory

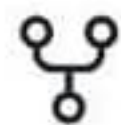
Comment

Maintainers can decide whether to accept the reported advisory, or close it.

Can it be reproduced? Is it in line with our security policy?



  security-researcher-1 added as a collaborator 1 minute ago



Collaborate on a patch in private

Use a temporary private fork of **octo-org/octo-repo** to collaborate on a fix.

Start a temporary private fork



Thank you for reporting a vulnerability.

Your report is being reviewed by **octo-org-octo-repo** owners. You will be notified if the report is published as an advisory.

Collaborate on a private fork with access controlled via the security advisory.

Enables any contributor to be given access to this fork via the advisory, so that they can work on/review the proposed fixes.



Collaborate on a patch

HTTPS

SSH

GitHub CLI

`https://github.com/mautic/`



Use [the temporary private fork](#) to collaborate on a patch for this advisory.



#1 opened on 6 Dec 2024 by tomekkowalczyk

`mautic/mautic:6.x`



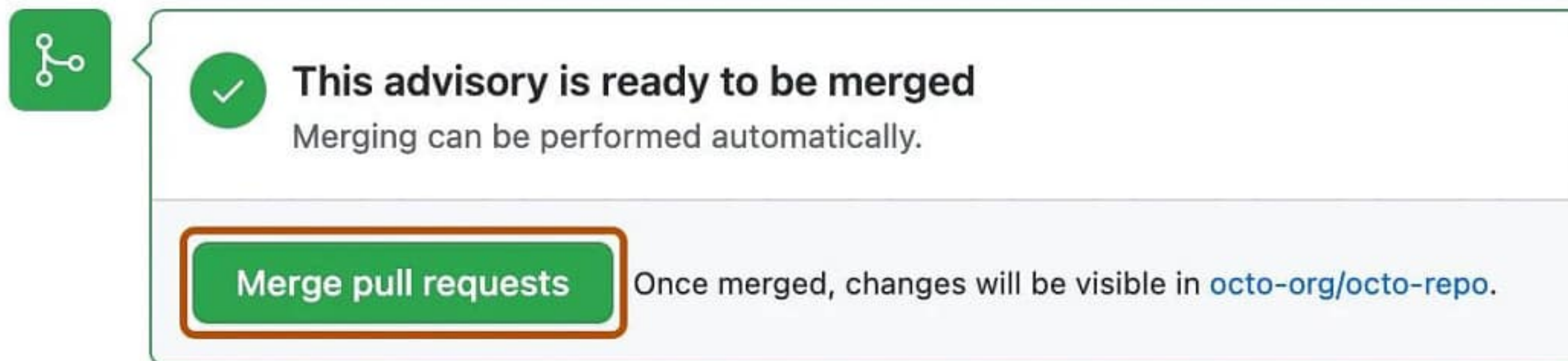
`mautic/`

Delete temporary private fork

**Exact same process as making a PR in your main repository,
but done privately.**

Collaborators clone the private fork, create a branch, and PR their changes as they normally would, which then shows in the advisory.





Merge all PRs relating to the advisory with a single click!

PRs on advisories are merged all at once, by clicking one button - this merges the commits directly to the branch in your main repository.



Merge pull request from [GHSA-mgv8-w49f-822w](#) 

 4 people authored on Apr 11, 2024 ·  53 / 53

Verified

b4b4ab5



Merge pull request from [GHSA-qjx3-2g35-6hv8](#) 

 4 people authored on Apr 11, 2024 ·  53 / 53

Verified

22bdd07



Merge pull request from [GHSA-jj6w-2cqq-7p94](#) 

 3 people authored on Apr 11, 2024 ·  51 / 53

Verified

e75b1ee



Merge pull request from [GHSA-9fcx-cv56-w58p](#) 

 4 people authored on Apr 11, 2024 ·  52 / 53

Verified

546045f



Merge pull request from [GHSA-2rc5-2755-v422](#) 

 3 people authored on Apr 11, 2024 ·  53 / 53

Verified

2d64839



Single squashed commit shows in your commit history.

Once the advisory is published (when you've released the fix) the commits link back to the original advisory, closing the loop for people checking the commit history.



The screenshot shows a GitHub Advisory credit interface. At the top, a user profile for 'RCheesley Ruth Cheesley' is visible. Below it, a vertical list of credits is shown, each with an icon (person or trophy) and a description. A dropdown menu is open on the right, titled 'Choose a credit type' with a checkmark. The menu lists the following credit types: Analyst, Finder, Reporter, Coordinator, Remediation developer, Remediation reviewer, Remediation verifier, Tool, Sponsor, and Other. A mouse cursor is pointing at the 'Choose a credit type' header.

○ **RCheesley** Ruth Cheesley

added themselves as a collaborator

was credited as a reporter on Dec 26

was credited as an analyst on Dec

✓ Choose a credit type

- Analyst
- Finder
- Reporter
- Coordinator
- Remediation developer
- Remediation reviewer
- Remediation verifier
- Tool
- Sponsor
- Other

Ensure that everyone involved in the security issue is credited on the advisory.

It takes a village ... with the GitHub Advisories you can recognise that by crediting everybody involved, even tools and sponsors.



Eta vulnerable to Code Injection via templates rendered with user-defined data

High severity

GitHub Reviewed

Published last week to the GitHub Advisory Database • Updated 17 hours ago

Vulnerability details

Dependabot alerts 7

Package

 eta (npm)

Affected versions

< 2.0.0

Patched versions

2.0.0

Dependabot alerts automatically inform repositories which have your project as a dependency.

A PR is provided to bump the version to the patched release, alerts show on the advisory itself in a separate tab.







<https://mau.tc/github-advisories>





With GitHub Advisories we can now ...

- Have a centralised location for all things security
- Invite contributors to work on fixes themselves, rather than *have* to do all the work ourselves
- Ensure that reports contain the minimum set of information required for CVE submission
- Simplify the merging of security fixes affecting multiple branches with a 'one click merge'





GitHub Advisories solved 95% of our pain points, except ...

- You can't (currently) run your GitHub Actions on a private fork in GitHub
- Merging multiple advisories in one release is still very time consuming due to the need to run automated tests after each is merged
- You can't auto-assign a team to access every new advisory, only admins get access by default
- Requesting/updating CVEs is manual for CNAs
- You can't PR to a different repo (e.g. an extended long term support private repo) from an advisory, only the main public repo - still some manual git-fu needed.







Ruth Cheesley (she/her)

What questions can I answer?

ruth.cheesley@mautic.org

speaking.ruthcheesley.co.uk for slides, recording,
links and resources