Open redirect vulnerability via endpoint authorize_and_redirect/?redirect= in posthog/posthog

0

✓ Valid Reported on Mar 22nd 2022

Description

Posthog application is vulnerable to open redirect which can be exploited by adding authorize_and_redirect/?redirect=https://evil.com endpoint.

Proof of Concept

1.Open the link https://app.posthog.com/login?next=/authorize_and_redirect/%3Fredirect%3Dhttps%25253A%25252F%25252Fevil.com
2.Login with your account and click on "Authorize None"
3.Now you will see you will get redirected to https://evil.com/

Video PoC

https://drive.google.com/file/d/1NIG6_wM0SAKlKEjOxVuKF2UbI8Xs16s8/view?usp=sharing

Impact

Url Redirection or Unvalidated Open Redirects are usually used with phishing attacks or in malware delivery, it may confuse the end-user on which site they are visiting.
1.Attackers could redirect victims to vulgar sites such as 18+ sites which can degrade the reputation of your site, as the redirection happened from your domain.
2.Attackers could deliver malware or phishing pages in the name of your website & hence cab steal user credentials.

Occurrences

decide.py L34 urls.py L72

Chat with us

References

References

- mitre

CVE
CVE-2022-0645
(Published)

Vulnerability Type
CWE-601: Open Redirect

Severity
Medium (6.1)

Visibility
Public

Status
Fixed

Found by

SAMPRIT DAS
@sampritdas8
pro

This report was seen 807 times.

We are processing your report and will contact the **posthog** team within 24 hours. 8 months ago

We have contacted a member of the **posthog** team and are waiting to hear back 8 months ago

We have sent a follow up to the **posthog** team. We will try again in 7 days. 8 months ago

A **posthog/posthog** maintainer modified the report 8 months ago

SAMPRIT DAS modified the report 8 months ago

SAMPRIT DAS 8 months ago Researcher

Hello @maintainer,

Chat with us

The CVSS score is not low it should be medium you can see all those below reports for open redirect all are given CVSS as 7.1 /6.1 medium:-

redirect all are given CVSS as 7.1/6.1 medium.

https://huntr.dev/bounties/4fb42144-ac70-4f76-a5e1-ef6b5e55dc0d/
https://nvd.nist.gov/vuln/detail/CVE-2021-38123

https://nvd.nist.gov/vuln/detail/CVE-2020-11053
https://nvd.nist.gov/vuln/detail/CVE-2018-1000671
https://nvd.nist.gov/vuln/detail/CVE-2022-0597

SAMPRIT DAS 8 months ago Researcher

@admin Can you please ask @maintainer to allow you to assign a CVE for this report?

Jamie Slome 8 months ago Admin

@sampritdas8 - please allow the maintainer to make their assessment before requesting a CVE. If they do not believe the report to be valid, we will not assign a CVE in any case.

A posthog/posthog maintainer 8 months ago Maintainer

We have implemented a fix that limits the redirect to the referer.
https://github.com/PostHog/posthog/pull/9268

Our reason for assigning this low was that the user specifically had to click that they wanted to be redirected to the evil site with a big warning.

SAMPRIT DAS 8 months ago Researcher

Thanks for the fix @maintainer. Actually, users will think the link evil.com is trusted because it is attached to your domain and they will click on it.

SAMPRIT DAS modified the report 8 months ago

SAMPRIT DAS 8 months ago Researcher

@admin as the maintainer has deployed the fix can you please validate the report and merged the fix as I can see also in the report:- https://huntr.dev/bounties/6961d738-60e4-461a-acd3-e276d422070f/ maintainer is facing problem for validating the report.

Chat with us

SAMPRIT DAS 8 months ago Researcher

@admin Now can you please assign a CVE for this report?

SAMPRIT DAS modified the report 8 months ago

SAMPRIT DAS modified the report 8 months ago

SAMPRIT DAS 8 months ago Researcher

@admin

Jamie Slome 8 months ago Admin

@sampritdas8 - please do not spam the @admin tag. Excessive usage will result in the disabling of this action for your account.

Please allow the maintainer to approve and confirm the fix, as they may have their own schedule on making this report public and releasing the fix.

@maintainer - let me know if you are having any issues and I can support you. @sampritdas8 please be patient and wait for the maintainer to respond.

A posthog/posthog maintainer modified the report 8 months ago

A posthog/posthog maintainer validated this vulnerability 8 months ago

SAMPRIT DAS has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A posthog/posthog maintainer marked this as fixed in master with commit 859d8e
8 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

urls.py#L72 has been validated ✓

decide.py#L34 has been validated ✓

Chat with us

SAMPRIT DAS 8 months ago Researcher

Sorry, @admin for disturbing you, now can you please assign a CVE for this report?

Jamie Slome 8 months ago Admin

Sure - @maintainer are you happy for us to assign and publish a CVE for this report?

A posthog/posthog maintainer 8 months ago Maintainer

Does publishing a CVE means this will be public? In that case we'd prefer waiting until the next release for this (~ 4 weeks) so self hosted users have a chance to update with a fix.

Jamie Slome 8 months ago Admin

Yes, when publishing a CVE, the report will be distributed into various intelligence databases including the NVD/MITRE.

A posthog/posthog maintainer 8 months ago Maintainer

In that case we'd like to keep this private until we have a new version available that allows self hosted users to update

Jamie Slome 8 months ago Admin

Sure 👍 Would you like me to also make the report itself private on our platform, as it is currently public.

A posthog/posthog maintainer 8 months ago Maintainer

Yep, thanks

Jamie Slome 8 months ago Admin

Done! ✅

Chat with us

SAMPRIT DAS 8 months ago Researcher

@maintainer please update us once the new version has been released

SAMPRIT DAS 8 months ago Researcher

@admin, it can be possible that for now, you assign the CVE once the new version has been released you can make the report public and can update the CVE on NVD/MITRE?

Jamie Slome 8 months ago Admin

Sure, we can assign the CVE now and wait to publish it once the report is ready to go live.

@maintainer - thoughts?

SAMPRIT DAS 8 months ago Researcher

@maintainer what is your decision?

SAMPRIT DAS 8 months ago Researcher

Admin as the report is
Severity:
Medium (6.1)

Still, I have not received any bounty why so?

A posthog/posthog maintainer 8 months ago Maintainer

Not sure I understand the question. We don't want to publish anything before the new release.

SAMPRIT DAS 8 months ago Researcher

@maintainer Admin wants to say that he will assign the CVE number to this report and it will get published once the new release will take place.

Jamie Slome 8 months ago Admin

@sampritdas8 - let's leave this report as it is until we take it live.

With regards to the bounties, we do not reward bounties on Medium severity reports against non-featured repositories.

If you have any more questions, please get in touch via security@huntr.dev or join our Discord.

SAMPRIT DAS 8 months ago Researcher

Okay admin

SAMPRIT DAS 8 months ago Researcher

@maintainer I have retested your application and confirmed that the vulnerability has been fixed and a new release is out now can you give permission to @admin to assign a CVE to this report and to disclose the report?

SAMPRIT DAS 8 months ago Researcher

@admin https://github.com/PostHog/posthog/pull/9268 here you can see the fix has been released on version 1.34.0 so can you assign the CVE and disclose the report?

Jamie Slome 8 months ago Admin

We will only do this with the go-ahead from the maintainer. Please wait to hear back from them here.

SAMPRIT DAS 8 months ago Researcher

@maintainer Can you please respond?

SAMPRIT DAS 8 months ago Researcher

@admin they are not replying can you please ask them? and have confirmed

Jamie Slome 8 months ago Admin

As mentioned above, please wait for the maintainers to respond 👍

Harry Waye 7 months ago Maintainer

@admin we have released, happy to assign a CVE here. Is there anything else required here e.g. how might I provide mitigation steps e.g. upgrade to 1.34.x?

SAMPRIT DAS 7 months ago Researcher

@admin Maintainer has given permission so can you now assign CVE, update it on nvd, and make the report public?

Jamie Slome 7 months ago Admin

Sure, I will get a CVE assigned and published here.

@Harry, there is nothing else required from your side :) Thanks for the contributions all!

SAMPRIT DAS 7 months ago Researcher

Thank you @admin and @Harry

Jamie Slome 7 months ago Admin

Assigned and published 👍

SAMPRIT DAS 7 months ago Researcher

@admin The report is still private can you please make it public?

Jamie Slome 7 months ago Admin

Sorted 👍

Chat with us

Sign in to join this conversation

Chat with us