

Cross-site Scripting (XSS) - Reflected in hestiacp/hestiacp

0



Valid

Reported on Mar 2nd 2022

Description

Please enter a description of the vulnerability.

Proof of Concept

```
xss in function add domain
POST /add/web
v-custom-doc-domain=<script>alert(1)</script>
https://drive.google.com/file/d/1EeoOX7Pmn5ptuweine4Cgcy1fyd6qEzJ/view?usp=
```



Impact

CVE

CVE-2022-0838

(Published)

Vulnerability Type

CWE-79: Cross-site Scripting (XSS) - Reflected

Severity

Medium (6.6)

Visibility

Public

Status

Fixed

Found by



huydoppa

Chat with us



@huydoppa

unranked ▼

This report was seen 671 times.

We are processing your report and will contact the **hestiacp** team within 24 hours. 9 months ago

Jaap Marcus validated this vulnerability 9 months ago

huydoppa has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Jaap Marcus 9 months ago

Maintainer

@admin please assign a CVE for this issue

Jamie Slome 9 months ago

Admin

CVE assigned (**CVE-2022-0838**)! 🎉

Jamie Slome 9 months ago

Admin

Please ping me once you are ready to publish the fix and make the report public, and I will publish the CVE to MITRE.

huydoppa 9 months ago

Researcher

<https://www.huntr.dev/bounties/8ce4b776-1c53-45ec-bc5f-783077e2d324/> have 10\$ for report

Jaap Marcus 9 months ago

Maintainer

Rules have changed and Huntr.dev doesn't pay anything for Medium or Low CSV score on non featured ones ... Due to complains from maintainers. See Huntr.dev discord channel

Chat with us

Jaap Marcus 9 months ago

Maintainer

Bug was present in a javascript function that displays the domain didn't sanitise it...

Jaap Marcus marked this as fixed in 1.5.10 with commit 640f82 9 months ago

The fix bounty has been dropped ❌

This vulnerability will not receive a CVE ❌

Jamie Slome 9 months ago

[Admin](#)

CVE published! 🇺🇸

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us