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

0

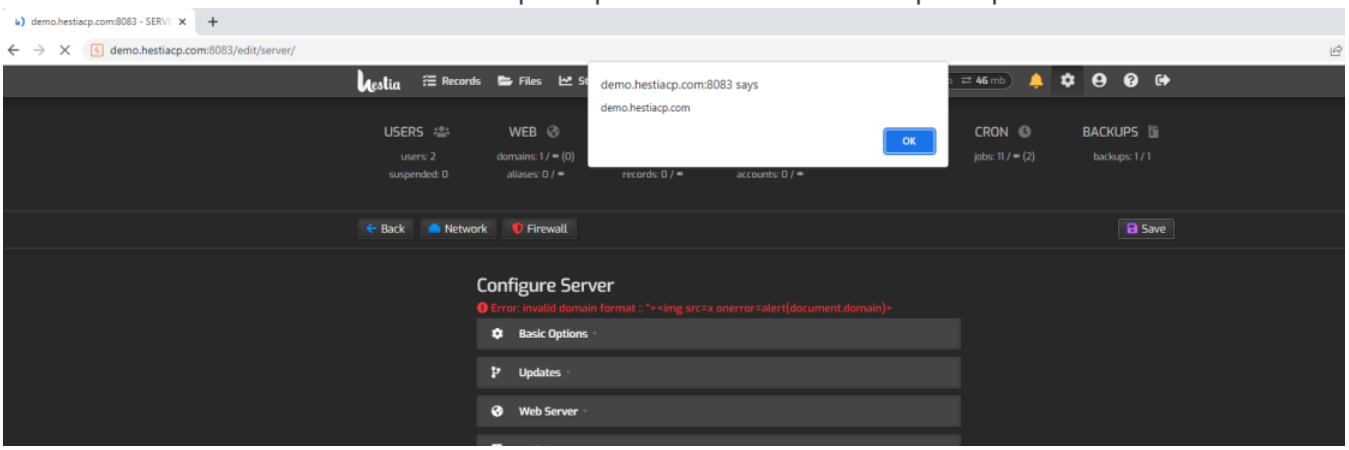
Valid Reported on Mar 9th 2022

Description

hestiacp is vulnerable to Reflected XSS in the Hostname field within Basic Options of the function "Configure Server" in Hestia Control Panel

Proof of Concept

(1) Access https://demo.hestiacp.com:8083/edit/server/
(2) Click "Configure"
(3) Click Basic Options
(4) Enter below as payload in the hostname field and click save
"><img src=x onerror=alert(document.domain)>
An attacker control alert box should prompt before an error box prompt from server.



Impact

This vulnerability is capable for letting attacker potentially steal a user's cookie and gain unauthorized access to that user's account through the stolen cookie.

CVE
CVE-2022-0986

(Published)

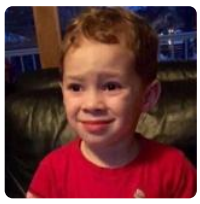
Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Reflected

Severity
Low

Visibility
Public

Status
Fixed

Found by



James Yeung
@scriptidiot
unranked

Fixed by

Jaap Marcus
@jaapmarcus
maintainer

This report was seen 716 times.

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

James Yeung modified the report 9 months ago

James Yeung modified the report 9 months ago

James Yeung modified the report 9 months ago

James Yeung modified the report 9 months ago

James Yeung 9 months ago Researcher

Modified the report for another function that is vulnerable to Reflected XSS, a
reported one is now fixed.

James Yeung modified the report 9 months ago

James Yeung modified the report 9 months ago

James Yeung modified the report 9 months ago

We have contacted a member of the **hestiacp** team and are waiting to hear back 9 months ago

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

James Yeung modified the report 8 months ago

Jaap Marcus modified the report 8 months ago

Jaap Marcus validated this vulnerability 8 months ago

James Yeung has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

James Yeung 8 months ago Researcher

@maintainer @admin
May I have CVE assigned for this case?

Jaap Marcus 8 months ago Maintainer

The XSS vulnerability is indeed successfully executed how ever document.cookie doesn't contain any private data that contains. Session ID or "Access" Cookies.

Session cookies are always managed via our own "php-fpm" install as it always supposed to run on port 8083.

https://github.com/hestiacp/hestiacp/blob/fd42196718a6fa7fe17b37fab0933d3cbcb3db0d/src/deb/php/php-fpm.conf#L36-L37

Jamie Slome 8 months ago

Before assigning a CVE, we do require the 👍 from the maintainer.

Jaap Marcus 8 months ago Maintainer

@admin please go a head

Jamie Slome 8 months ago Admin

Sorted! ♥

`CVE-2022-0986` - please ping me once this is ready to be published + fixed 👍

Jaap Marcus marked this as fixed in 1.5.11 with commit fd4219 8 months ago

Jaap Marcus has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Jamie Slome 8 months ago Admin

CVE published! 🎊 It should be available in the MITRE/NVD databases shortly.

Sign in to join this conversation