

Sign in

hev0x / CVE-2021-26084_Confluence

Public

Notifications

Fork 81

Star 306

<> Code

Issues 2

Pull requests

Actions

Projects

Security

Insights

main

Go to file

<> Code

Confluence_OGNLInj...

README.md

README

CVE-2021-26084 - Confluence Server Webwork OGNL injection

- An OGNL injection vulnerability exists that would allow an authenticated user and in some instances unauthenticated user to execute arbitrary code on a Confluence Server or Data Center instance.

IMPORTANT

This exploit is only intended to facilitate demonstrations of the vulnerability by researchers. I disapprove of illegal actions and take no responsibility for any malicious use of this script. The proof of concept demonstrated in this repository does not expose any hosts and was performed with permission.

About

Confluence Server Webwork OGNL injection

Readme

Activity

306 stars

2 watching

81 forks

Report repository

Releases

No releases published

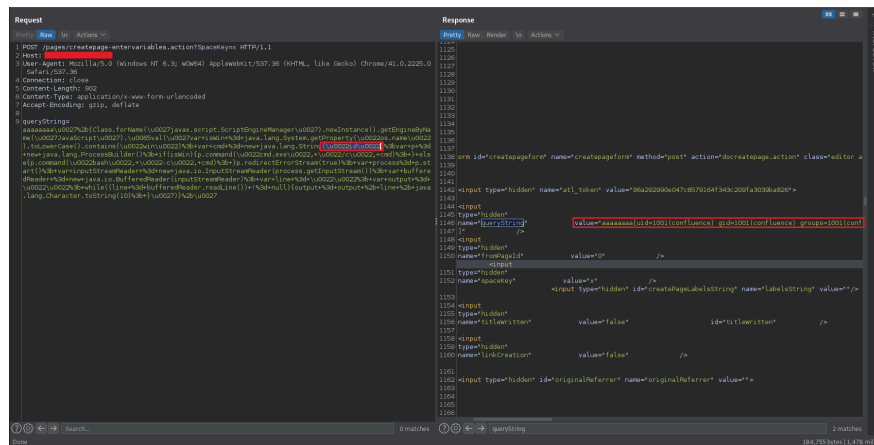
Packages

No packages published

Contributors 3

Languages

• queryString param Request



Python 100.0%

Exploit Usage

Commands:

```
$ python3 Confluence_OGNLInjection.py -u
```

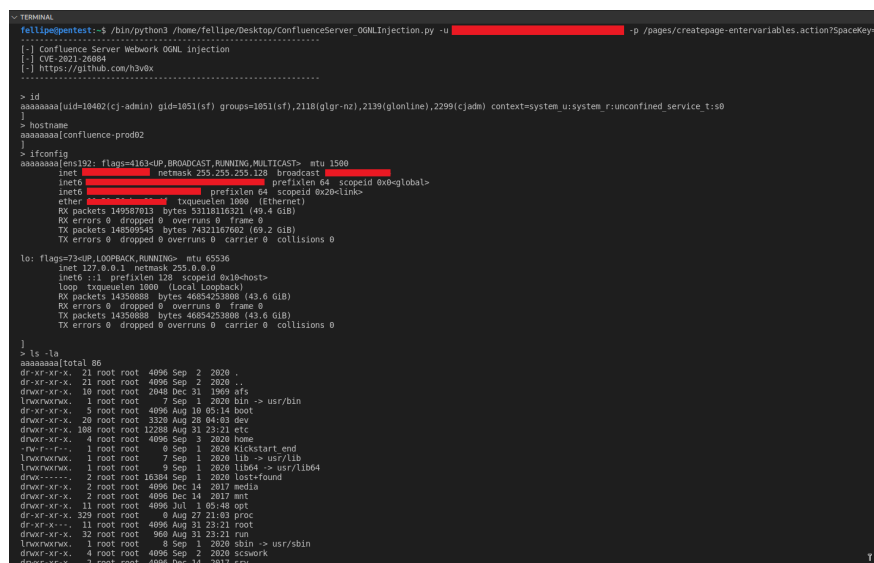
```
http://xxxxx.com
```

or

```
$ python3 Confluence_OGNLInjection.py -u
```

```
http://xxxxx.com -p /pages/createpage-entervariables.action?SpaceKey=x
```

• Exploitation with Confluence_OGNLInjection.py



- References:

<https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-1077906215.html>

<https://github.com/httpvoid/writeups/blob/main/Confluence-RCE.md>

<https://www.exploit-db.com/exploits/50243>

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.