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

TesterCC 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

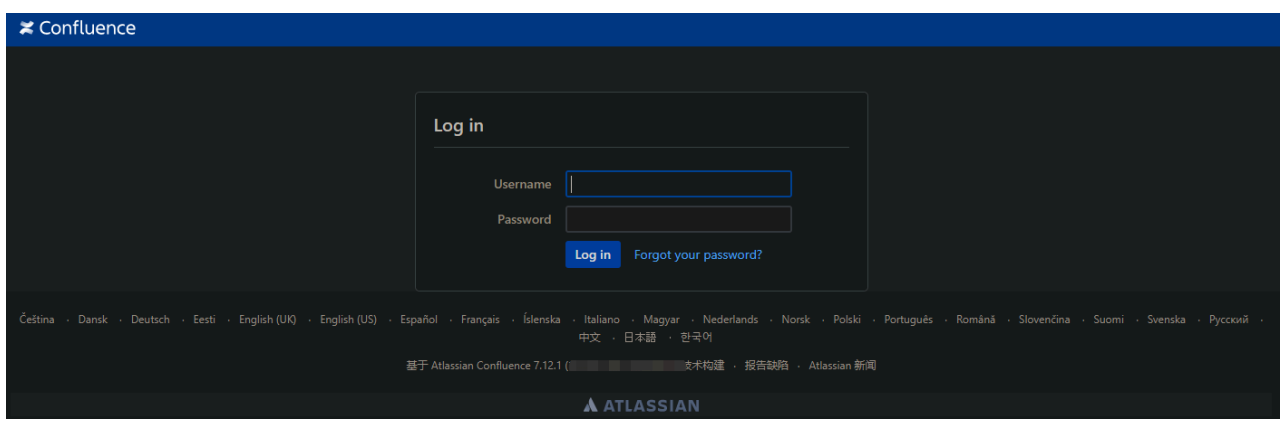
8月25 日，Atlassian官方发布了Confluence Server Webwork OGNL 注入漏洞的风险通告，漏洞 CVE 编号：CVE-2021-26084。经过身份验证的攻击者能利用该漏洞在目标系统上执行任意代码。目前官方已修复该漏洞，建议受影响用户及时更新至安全版本进行防护，做好资产自查以及预防工作，以免遭受黑客攻击。

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
```

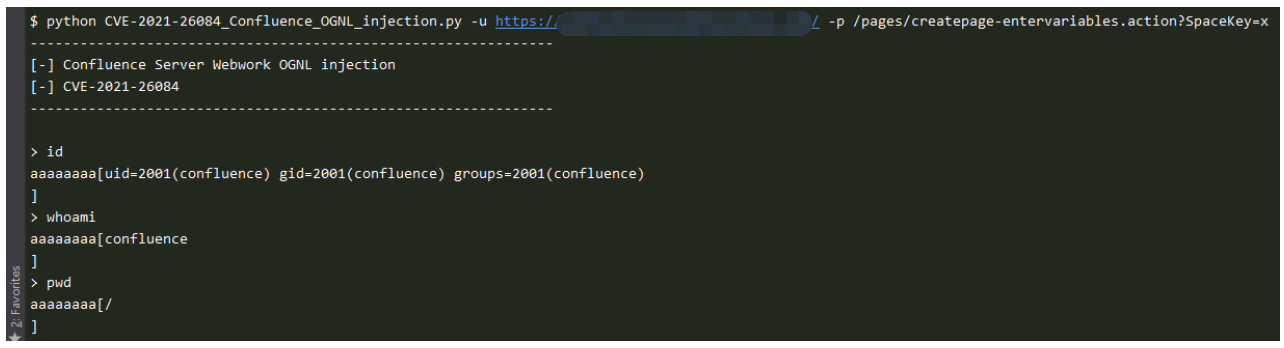


Search

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`



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，参考链
https://confluence.atlassian.com/doc/confluence-security-advisory-2021-0

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