BackBox Test and Mitigation for CVE-2021-44228 And CVE-2021-45046 Vulnerabilities

Affected Products

BackBox versions 6.51.05 up to 6.53.x

Details

A flaw was found in the Java logging library Apache Log4j in versions from 2.0.0 and before as well as version 2.14.1. This allows a remote attacker to execute code on the server if the system logs an attacker-controlled string value with the attacker's JNDI LDAP server lookup.

Statement

This issue only affects log4j versions between 2.0 and 2.14.1. In order to exploit this flaw you need:

A remotely accessible endpoint with any protocol (HTTP, TCP, etc) that allows an attacker to send arbitrary data,

A log statement in the endpoint that logs the attacker-controlled data.

Due to the existence of JMS Appender which can use JNDI in the log4j 1.x, it is possible that log4j version 1.x is also affected by this vulnerability. The impact is still under investigation.

Mitigation

Run the following commands: (copy paste from link)

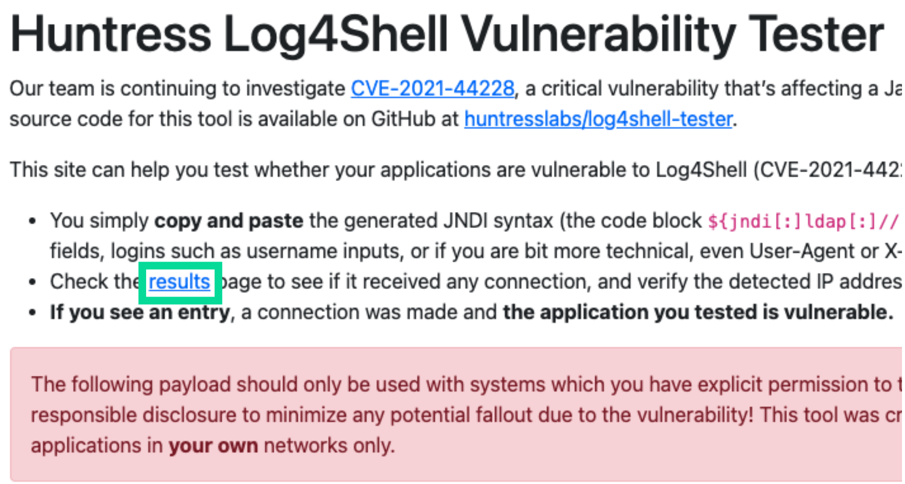
1. zip -q -d /backbox/backbox-3.0/app-server/apache-tomcat-7.0.37/webapps/ROOT/WEB-INF/lib/log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
2. service backbox stop
3. service backbox start

Prechecks

Instructions to test BEFORE applying the fix:

Pre-requisite: BackBox must be able to reach the internet for this test

1. Open your browser and navigate to: https://log4shell.huntress.com/
2. Click the results link



Huntress Log4Shell Vulnerability Tester

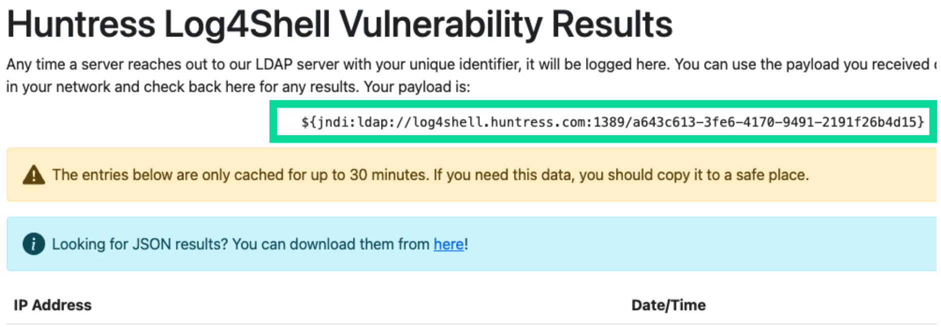
Our team is continuing to investigate CVE-2021-44228, a critical vulnerability that's affecting a Ja
source code for this tool is available on GitHub at huntresslabs/log4shell-tester.

This site can help you test whether your applications are vulnerable to Log4Shell (CVE-2021-442

- You simply **copy and paste** the generated JNDI syntax (the code block `${jndi[:]ldap[:]//`
fields, logins such as username inputs, or if you are bit more technical, even User-Agent or X-
- Check the results page to see if it received any connection, and verify the detected IP addres
- **If you see an entry**, a connection was made and **the application you tested is vulnerable.**

The following payload should only be used with systems which you have explicit permission to t
responsible disclosure to minimize any potential fallout due to the vulnerability! This tool was cr
applications in **your own** networks only.

3. Copy the payload



Huntress Log4Shell Vulnerability Results

Any time a server reaches out to our LDAP server with your unique identifier, it will be logged here. You can use the payload you received
in your network and check back here for any results. Your payload is:

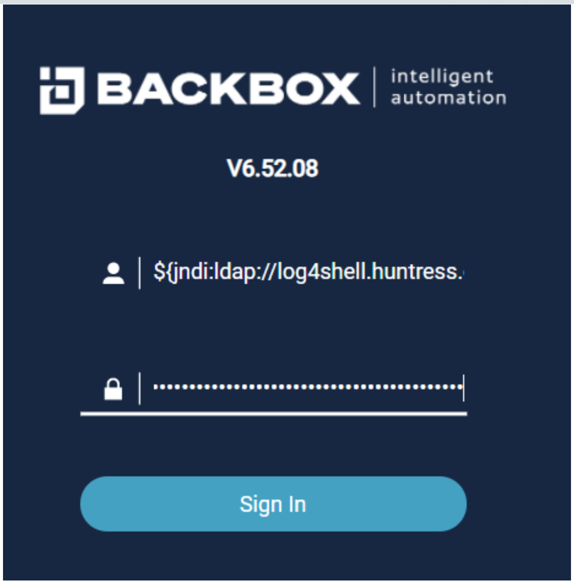
```
${jndi:ldap://log4shell.huntress.com:1389/a643c613-3fe6-4170-9491-2191f26b4d15}
```

⚠ The entries below are only cached for up to 30 minutes. If you need this data, you should copy it to a safe place.

ⓘ Looking for JSON results? You can download them from here!

IP Address	Date/Time

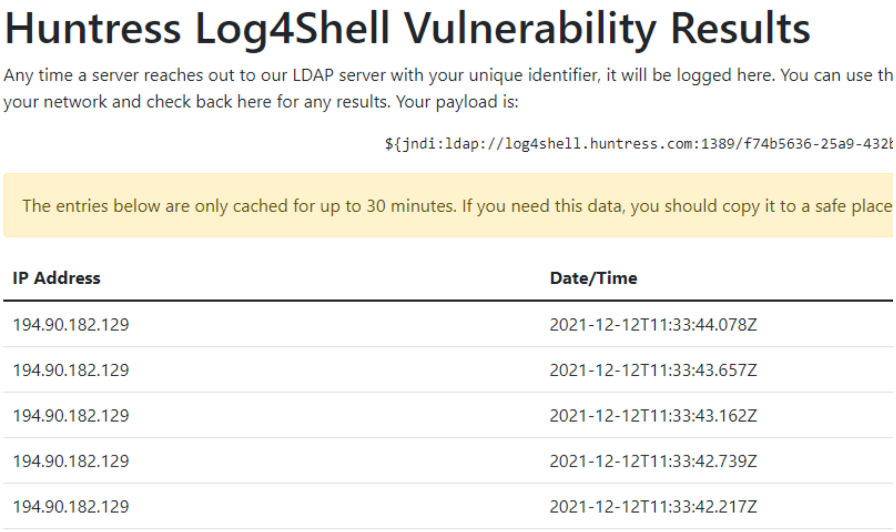
4. Open BackBox Web GUI in a new window and paste the payload in both the username and password fields and then click **Sign In**



${jndi:ldap://log4shell.huntress.

••

5. **Refresh the Huntress Log4Shell page and You should see one or more lines meaning BackBox is vulnerable.**



Huntress Log4Shell Vulnerability Results

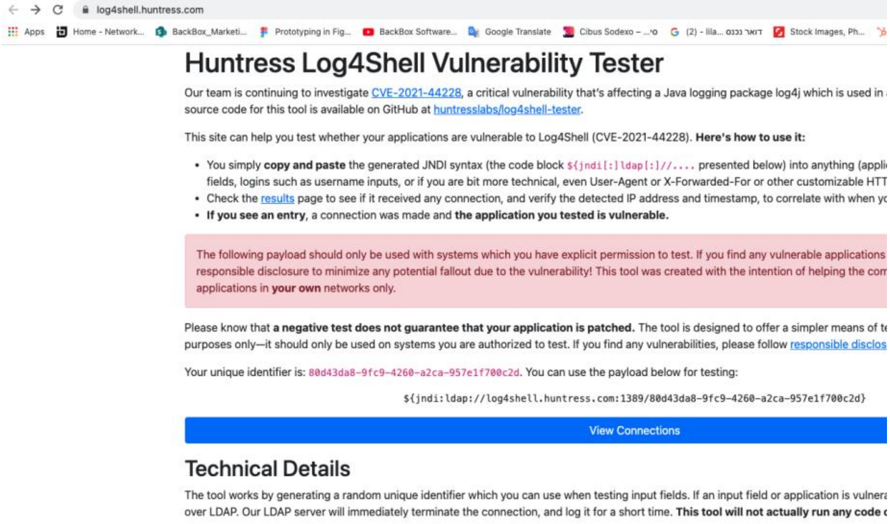
Any time a server reaches out to our LDAP server with your unique identifier, it will be logged here. You can use th your network and check back here for any results. Your payload is:

```
${jndi:ldap://log4shell.huntress.com:1389/f74b5636-25a9-432t
```

The entries below are only cached for up to 30 minutes. If you need this data, you should copy it to a safe place

IP Address	Date/Time
194.90.182.129	2021-12-12T11:33:44.078Z
194.90.182.129	2021-12-12T11:33:43.657Z
194.90.182.129	2021-12-12T11:33:43.162Z
194.90.182.129	2021-12-12T11:33:42.739Z
194.90.182.129	2021-12-12T11:33:42.217Z

6. Now click Back and refresh the page to get a new payload URL



log4shell.huntress.com

Huntress Log4Shell Vulnerability Tester

Our team is continuing to investigate CVE-2021-44228, a critical vulnerability that's affecting a Java logging package log4j which is used in
source code for this tool is available on GitHub at huntresslabs/log4shell-tester.

This site can help you test whether your applications are vulnerable to Log4Shell (CVE-2021-44228). **Here's how to use it:**

- You simply **copy and paste** the generated JNDI syntax (the code block `${jndi[:]ldap[:]//....` presented below) into anything (appli
fields, logins such as username inputs, or if you are bit more technical, even User-Agent or X-Forwarded-For or other customizable HTT
- Check the results page to see if it received any connection, and verify the detected IP address and timestamp, to correlate with when yo
- **If you see an entry**, a connection was made and **the application you tested is vulnerable.**

The following payload should only be used with systems which you have explicit permission to test. If you find any vulnerable applications
responsible disclosure to minimize any potential fallout due to the vulnerability! This tool was created with the intention of helping the com
applications in **your own** networks only.

Please know that **a negative test does not guarantee that your application is patched.** The tool is designed to offer a simpler means of te
purposes only—it should only be used on systems you are authorized to test. If you find any vulnerabilities, please follow responsible disclos

Your unique identifier is: `80d43da8-9fc9-4260-a2ca-957e1f700c2d`. You can use the payload below for testing:

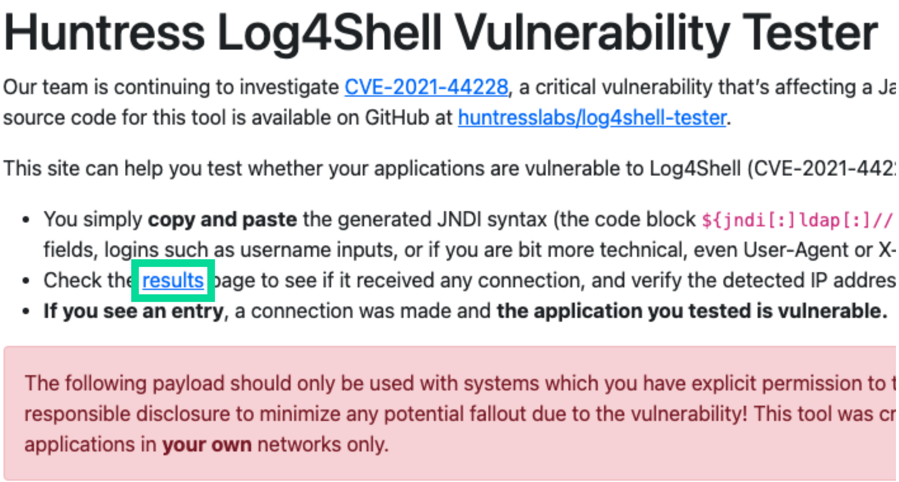
```
${jndi:ldap://log4shell.huntress.com:1389/80d43da8-9fc9-4260-a2ca-957e1f700c2d}
```

Technical Details

The tool works by generating a random unique identifier which you can use when testing input fields. If an input field or application is vulnera
over LDAP. Our LDAP server will immediately terminate the connection, and log it for a short time. **This tool will not actually run any code c**

7. Click the Results link and **MAKE SURE YOUR PAYLOAD URL IS NEW AND THERE ARE NO LINES FROM STEP 5**

8. **Copy your <u>NEW</u>** payload



Huntress Log4Shell Vulnerability Tester

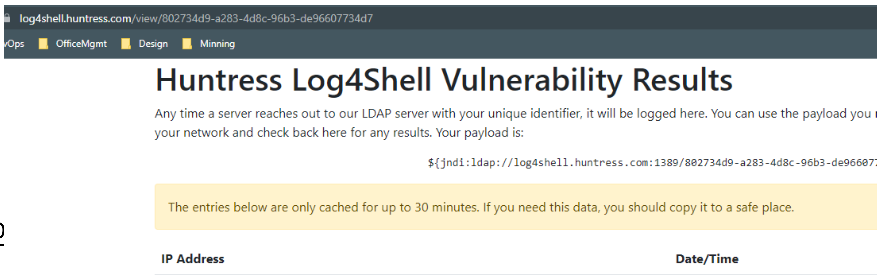
Our team is continuing to investigate CVE-2021-44228, a critical vulnerability that's affecting a Ja
source code for this tool is available on GitHub at huntresslabs/log4shell-tester.

This site can help you test whether your applications are vulnerable to Log4Shell (CVE-2021-442

- You simply **copy and paste** the generated JNDI syntax (the code block `${jndi[:]ldap[:]//`
fields, logins such as username inputs, or if you are bit more technical, even User-Agent or X-
- Check the results page to see if it received any connection, and verify the detected IP addres
- **If you see an entry**, a connection was made and **the application you tested is vulnerable.**

The following payload should only be used with systems which you have explicit permission to t
responsible disclosure to minimize any potential fallout due to the vulnerability! This tool was cr
applications in **your own** networks only.

9.



log4shell.huntress.com/view/802734d9-a283-4d8c-96b3-de96607734d7

Huntress Log4Shell Vulnerability Results

Any time a server reaches out to our LDAP server with your unique identifier, it will be logged here. You can use the payload you
your network and check back here for any results. Your payload is:

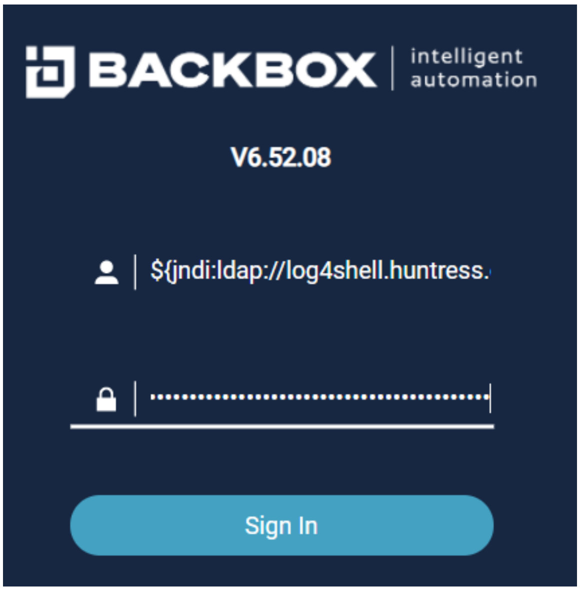
```
${jndi:ldap://log4shell.huntress.com:1389/802734d9-a283-4d8c-96b3-de96607
```

The entries below are only cached for up to 30 minutes. If you need this data, you should copy it to a safe place.

IP Address	Date/Time

Mitigation

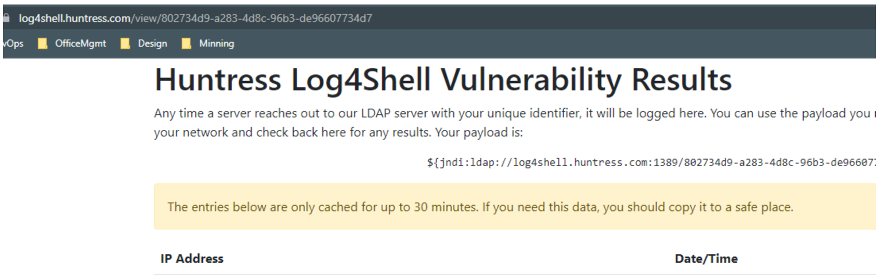
10. Connect to BackBox via SSH
11. Copy the commands from this text file and run them one by one: https://updates.backbox.com/V6.5/Docs/CVE-2021-44228&CVE-2021-45046.txt
12. Navigate to BackBox Web GUI again and enter the NEW PAYLOAD as username and password, Click Sign In



${jndi:ldap://log4shell.huntress.

••

13. The Results page should now remain without any entries, meaning we are no longer vulnerable.



log4shell.huntress.com/view/802734d9-a283-4d8c-96b3-de96607734d7

Huntress Log4Shell Vulnerability Results

Any time a server reaches out to our LDAP server with your unique identifier, it will be logged here. You can use the payload you ı your network and check back here for any results. Your payload is:

```
${jndi:ldap://log4shell.huntress.com:1389/802734d9-a283-4d8c-96b3-de96607
```

The entries below are only cached for up to 30 minutes. If you need this data, you should copy it to a safe place.

IP Address	Date/Time

For any questions, please don’t hesitate to contact us: support@backbox.com