CS 6035

Projects / Log4Shell / Flag 3: Config.Properties Surprise

FLAG 3: Config.Properties Surprise (25 pts)

Make sure you have gone through the Setup and Intro sections.

If you haven’t already, run the start script in the home directory of log4j user, start the container with the start script:

```
./StartContainer.sh
```

For this flag we will use the /cartoons/ resource. There are 4 total endpoints for this resource. Only the following 2 are relevant for this flag.

Call the following endpoint to fetch all the records. Save one of the ids.

GET All - Fetch all cartoon records:

```
curl 'http://localhost:8080/rest/cartoons/cartoonList' -H 'GATECH_ID:123456789'
```

Call the following endpoint to GET by ID and inspect the logged output.

GET By ID - Fetch a single cartoon record by ID:

```
curl 'http://localhost:8080/rest/cartoons/cartoon/<id>' -H 'GATECH_ID:123456789'
```

You have caught wind that there is a properties file that this application uses to inject configurable data during runtime.

For this exploit, you will use the log4j exploit to update the “config.properties” file saved in the root directory of the application. This properties file contains a property that will set the rating for all of the children’s cartoons.

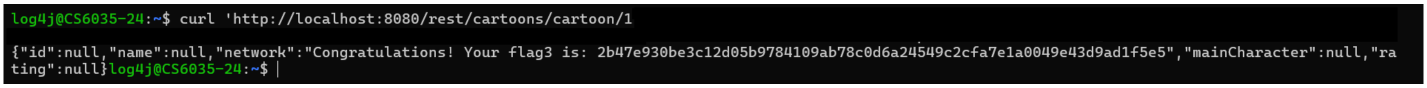
See if you can find anything that gives you a hint about how to exploit it/what you need to do, to update the property. Look for an out of place attack vector/variable.

This application links the properties’ rating to all children’s cartoons in its response. You have a beef with childrens cartoons and don’t think kids should watch cartoons. You want to set all of the ratings to R. Mean, catoons are great! However, first, you need to make sure that this is even possible.

One thing to keep in mind is that the application checks to see if this file has been tampered with. You will need to make sure you don’t overwrite the file and instead just update it. This means, all properties need to be as they were except the one you updated.

For this flag, you will need to update the properties file so that when the application builds the cartoon response, it sets the rating to your **gatechId**. *i.e. 123456789

If successful, you should get your flag in the network field of the response:



```
log4j@CS6035-24:~$ curl 'http://localhost:8080/rest/cartoons/cartoon/1

{"id":null,"name":null,"network":"Congratulations! Your flag3 is: 2b47e930be3c12d05b9784109ab78c0d6a24549c2cfa7e1a0049e43d9ad1f5e5","mainCharacter":null,"ra
ting":null}log4j@CS6035-24:~$ |
```

Note: The error message is simply informational and does not mean necessarily that your exploit was successfully executed or not.

Hint: Someone might have tried to roll their own patch and tried to deny requests containing malicious string patterns.
Hint: R rated cartoons are not exploitable.

***** IF THIS FLAG COMES OUT BLANK, Restart container by running the stopContainer and startContainer scripts in the home directory of the log4j user. *******

Disclaimer: You are responsible for the information on this website. The content is subject to change at any time.