Log4Shell Discovery Scanning

Self-Testing and Diagnosis - How to Guide (by Sean Murry-Ford, A2N CSO)

Overview:

CVE-2021-44228 (commonly known as Log4Shell) is a vulnerability which can cause Remote Code Execution (RCE) on certain versions and configurations of the Apache Software Foundation's logging service. This vulnerability can be exploited without authentication and has a CVSS score of 10. Although there are mitigations which can (and should) be applied, visibility and asset testing is important to ensure all vulnerable instances of *log4j* are discovered. Access2Networks (A2N) has developed a methodology for customers, partners and the public to assist with this process.

Log4Shell Exploit Process:

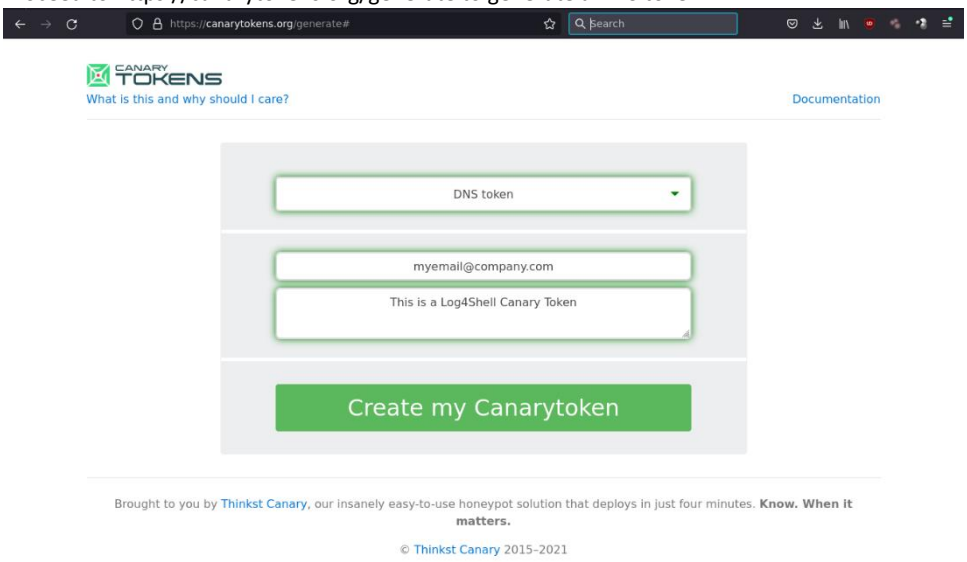
The exploit process requires the vulnerable software to make an LDAP connection to a threat actor-controlled LDAP server. This in turn will direct the log4j server to make a connection over HTTP/S which will then download and execute the malicious payload. This payload will run with the same privileges as the log4j process.

By utilizing Thinkst Canary Tokens DNS service combined with a custom script, customers, and partners of A2N will be able to perform their own testing which will create an e-mail alert if and when the script interacts with a vulnerable service.

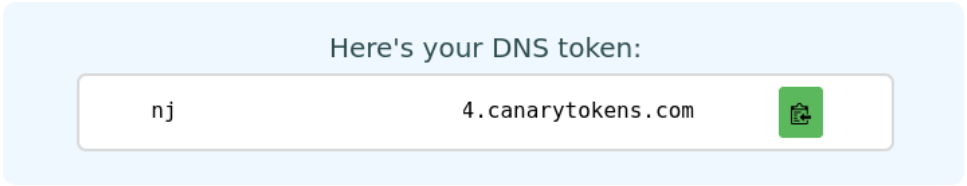
Detection Steps:

To properly detect the vulnerable services, please follow these steps:

1. Proceed to https://canarytokens.org/generate to generate a DNS token

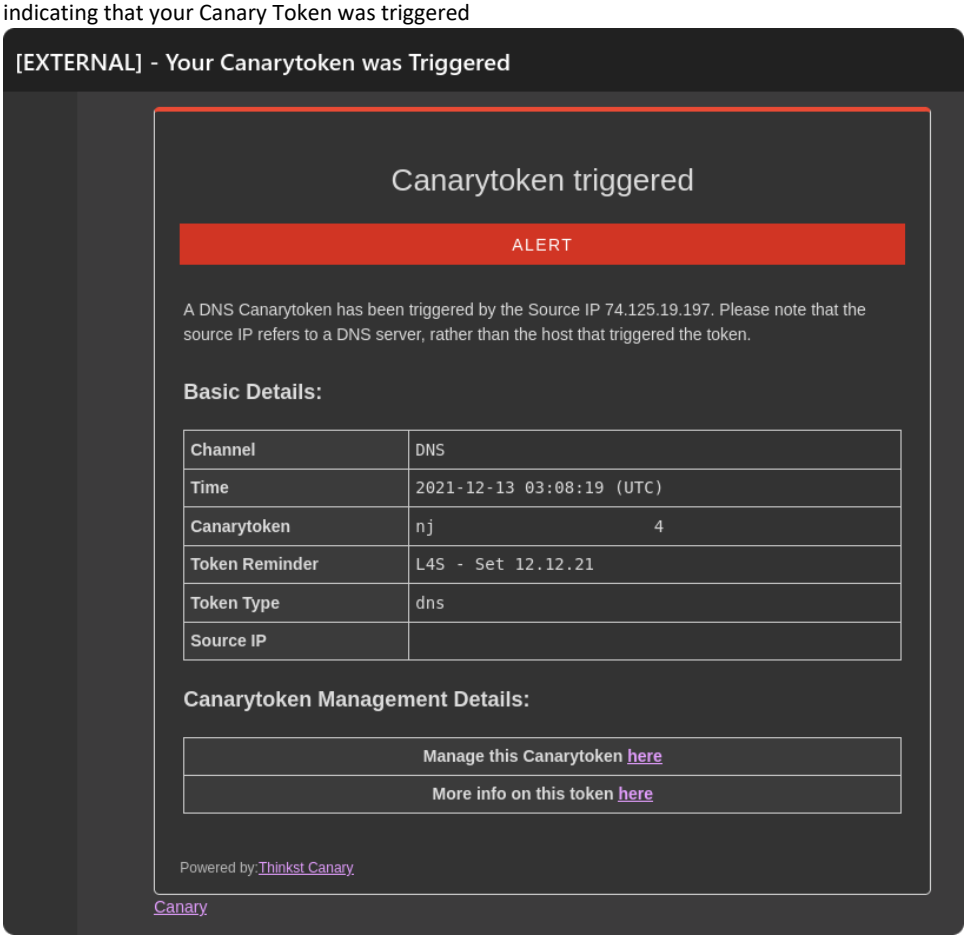


2. Once the token has been generated, take note of the FQDN provided to you



3. Download the script from A2N and modify the line which reads: CT="fixme" and replace "fixme" with the FQDN of your Canary Token you received in Step 2
4. [Optional] Modify the "TO" value to lengthen or shorten the timeout for each connection attempt (Default is 15 seconds)
5. Create a list of targets you would like to scan with each target listed on its own line with the IP/hostname followed by the port number similar to:
    i. 1.2.3.4:8080
    ii. mysite.com:1234
6. Ensure that all required ports are open from the scanning machine to your target hosts and ports you've created in your file from Step 5

7. Make the script executable with: chmod +x ./l4s_check.sh
8. Finally, run the script with: ./l4s_check.sh <input_file.txt>
a. Replace <input_file.txt> with the name of your actual input file
9. If a vulnerable service is hit, a DNS request will be made for the FQDN of your Canary Token and you will receive an e-mail indicating that your Canary Token was triggered



10. Should you receive an e-mail notification, you will need to investigate your DNS servers to see which computer made the request at that specific time as this indicates a vulnerable service

Should you require any assistance from A2N, please contact your Account Executive or our sales department - E: sales@a2n.net or Ph: 905-795-1711

Downloadable Script:

A2N has a script which is to be used in conjunction with Thinkst Canary Tokens to assist in detection of any vulnerable log4j instances. The script and all updates to it can be found here: https://pastebin.com/XaQZYbM2