CVE-2021-44228

Explanation

This Security Alert addresses CVE-2021-44228, a remote code execution vulnerability in Apache Log4j. It is remotely exploitable without authentication, i.e., may be exploited over a network without the need for a username and password.

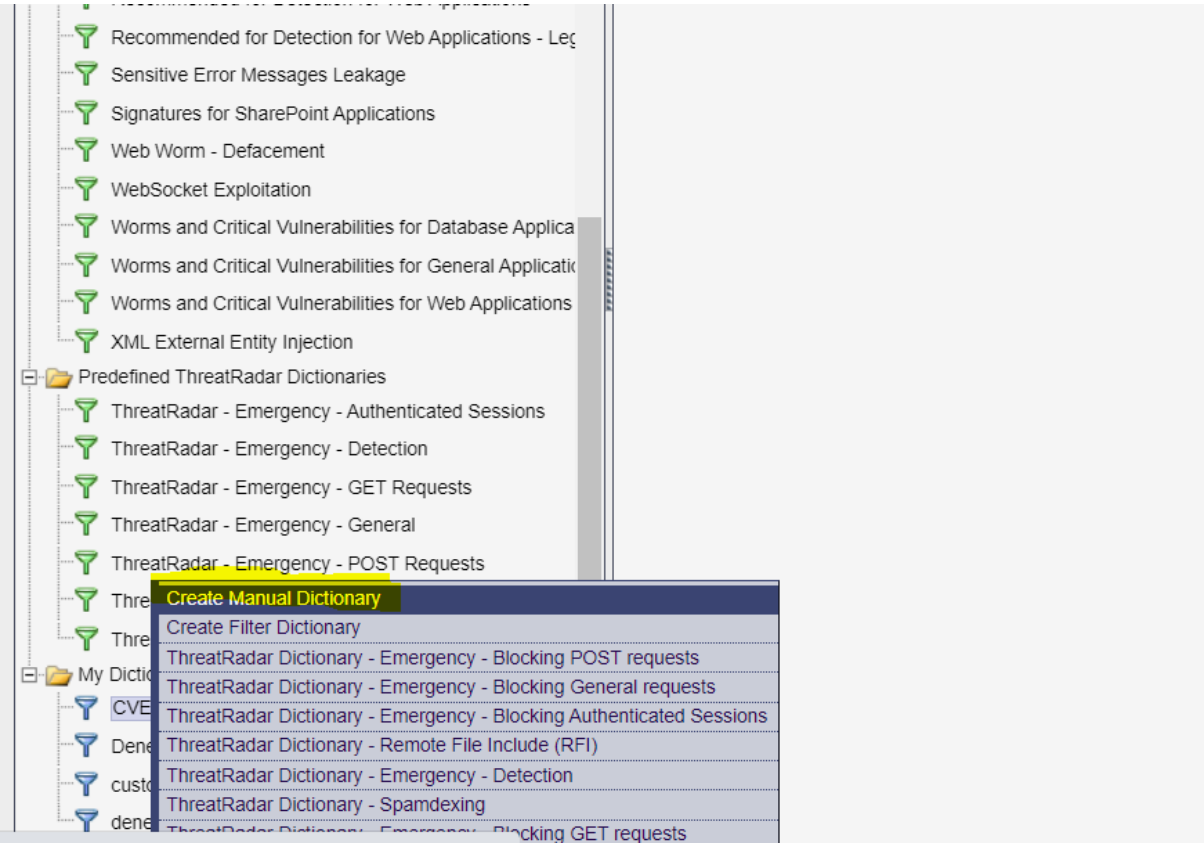
Severity

High

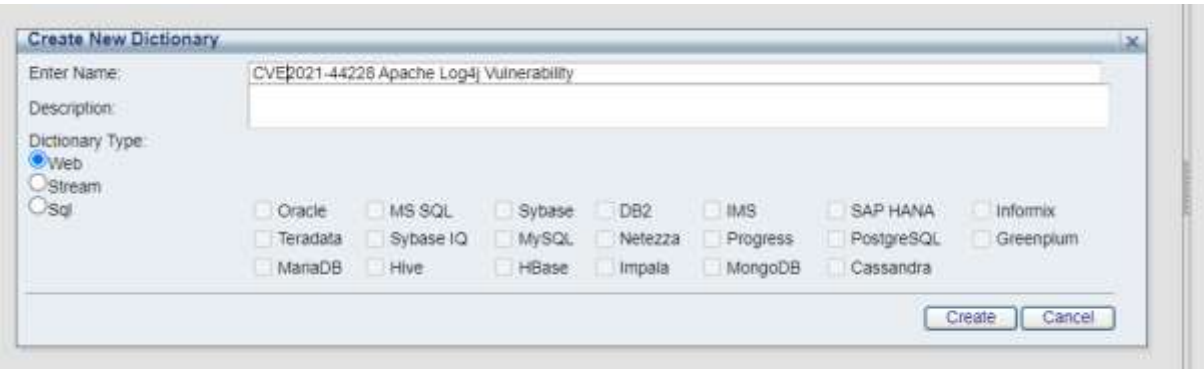
Precautions for Imperva WAF

1. Custom Dictionary creation

➔ Setup>Signatures tabs are followed
➔ Right click on the my dictionaries icon at the bottom of the left panel and select “create manual dictionary”.



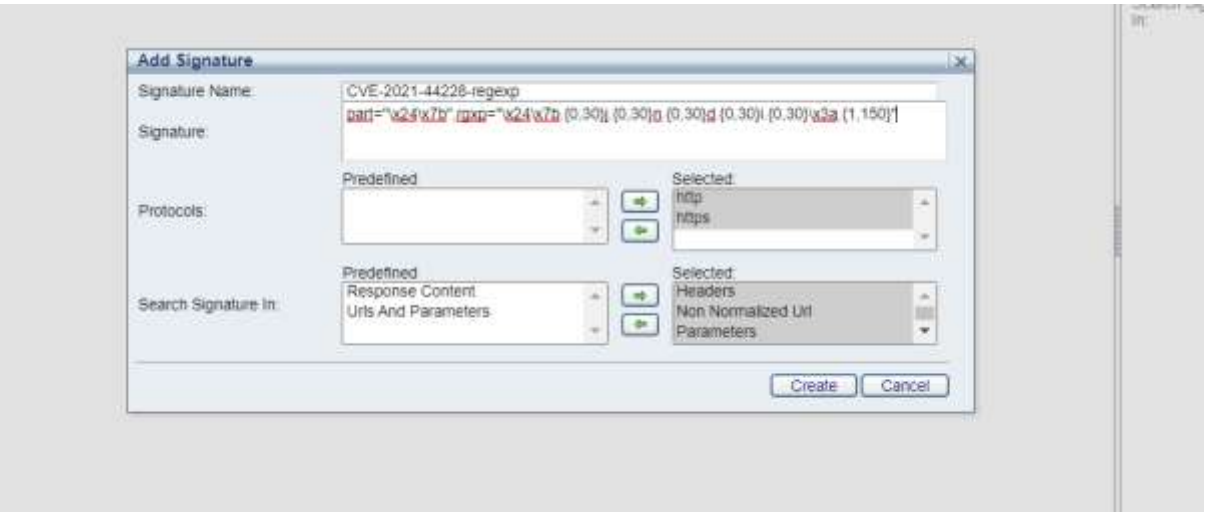
➔ In the panel that opens, the name of the related vulnerability is entered and web is selected as the type.

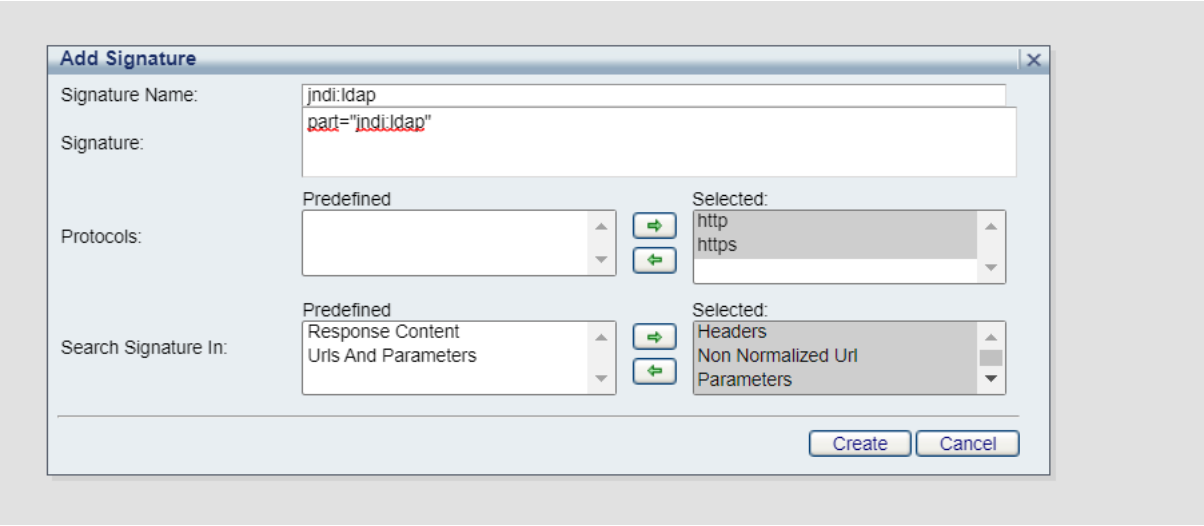


➔ After clicking the Create option, the dictionary is created.

➔ In the next step, 4 signatures with the names “jndi:dns” , “jndi:ldap” , “jndi:rmi” and CVE-2021-44228-regexp, which are used in vulnerability payloads, are created in the dictionary we have previously created.

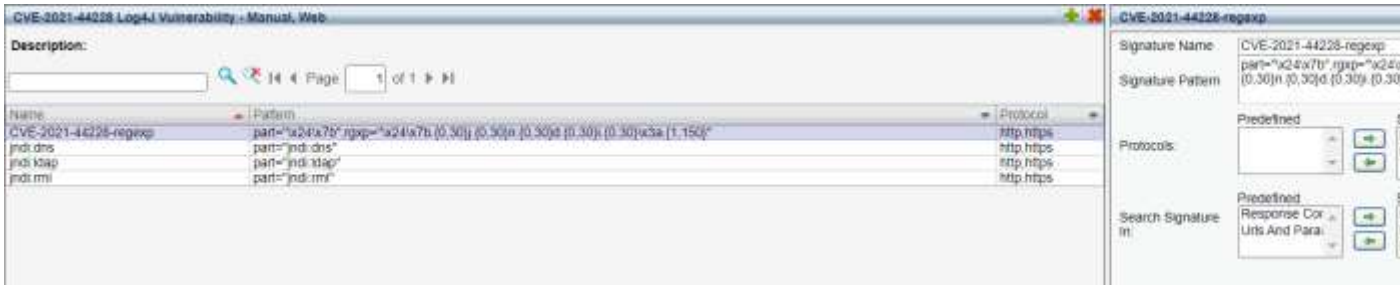
- When creating a signature here, signature part="jndi:ldap" for "jndi:ldap" and part="jndi:dns" for "jndi:dns" and part="jndi:rmi" for jndi:rmi should be written.
- For the CVE-2021-44228-regexp signature, it should be part="\x24\x7b",rgxp="\x24\x7b.{0,30}j.{0,30}n.{0,30}d.{0,30}i.{0,30}\x3a.{1,150}"
- HTTP and https should be selected as Protocols.
- In Search signature in section, Parameters,Request body,URL,Headers,Non-Normalized URL should be selected.





➔ A signature is created with the Create button

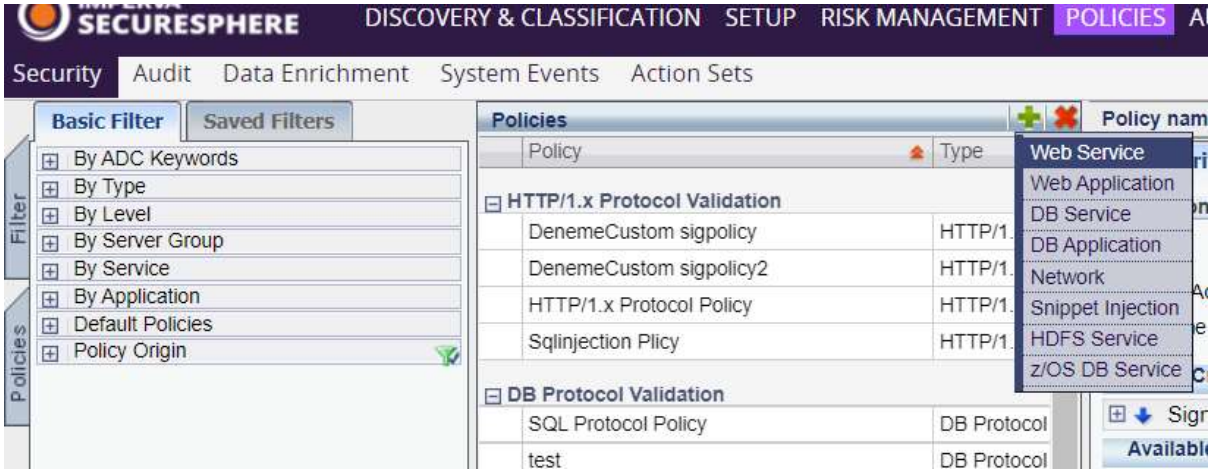
➔ The final image should be as follows.



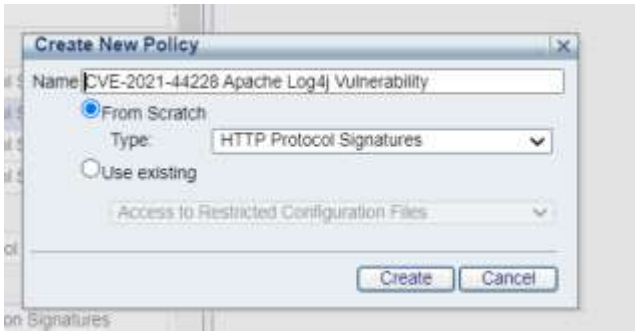
2. Web Service Policy creation

➔ Policies>Security tabs are followed

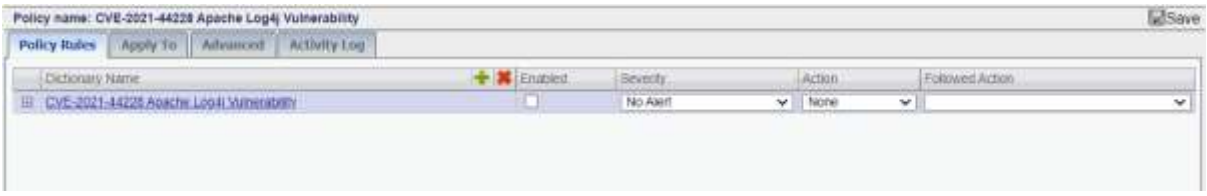
➔ By pressing the + button, web service is selected from the options.



➔ In the opened tab, the name of the related vulnerability is written and http protocol signatures is selected as the type.



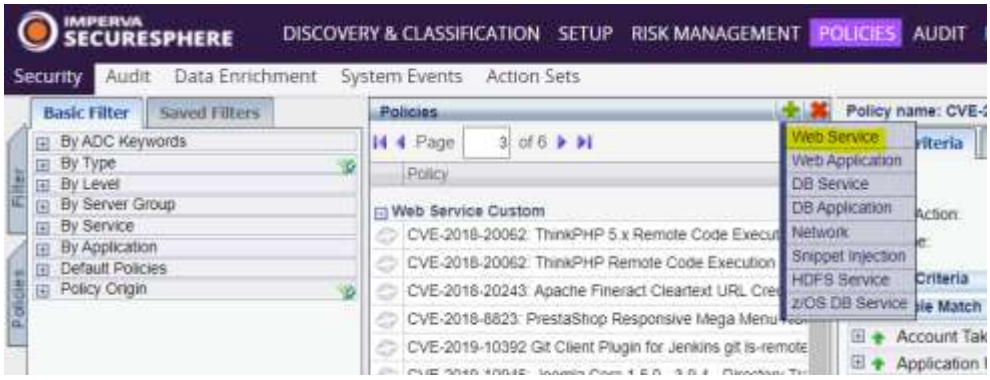
➔ By pressing the + button in the Policy Rules tab, the dictionary we created in the 1st step is selected. The final state should be the same as the screenshot. So Severity should be no alert and action should be none.



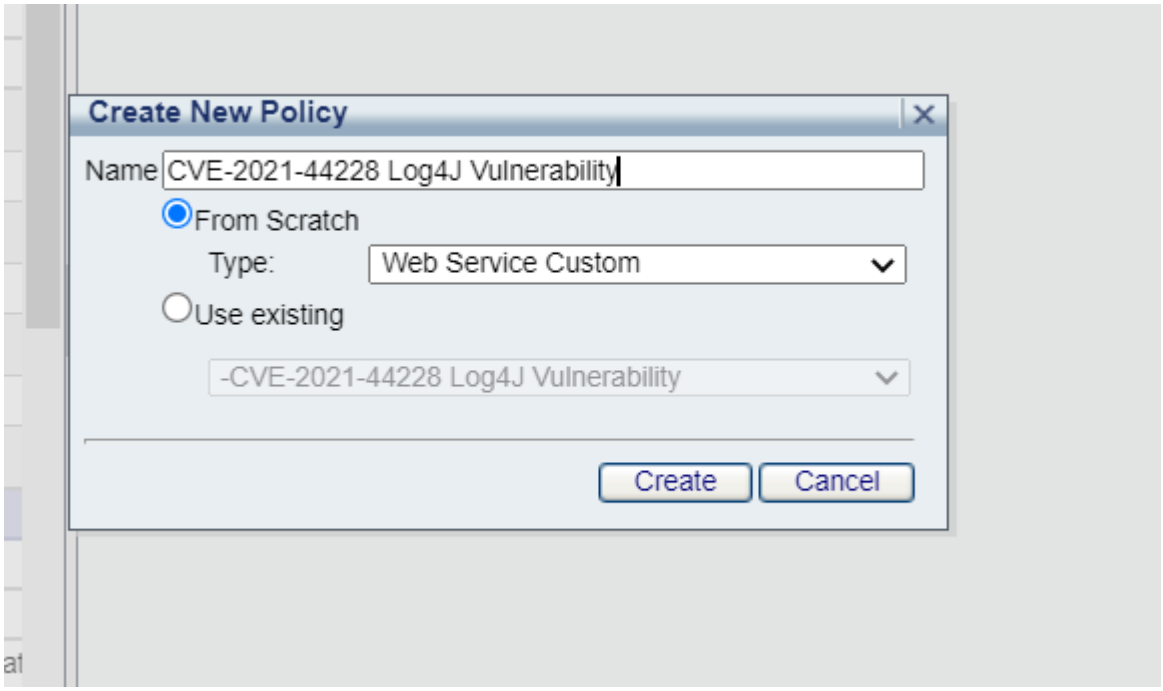
➔ After saving the changes, the policy is assigned to the relevant services from the apply to tab.

3. Creating a Web Service custom policy

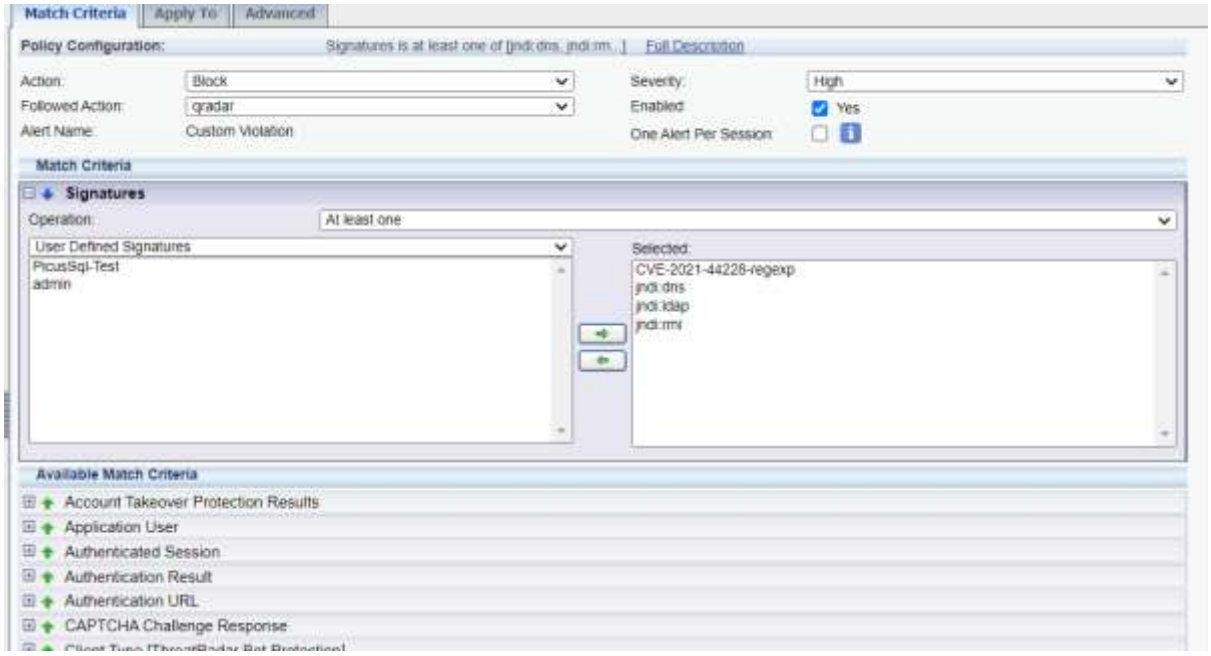
➔ Policies>Security tabs are followed
➔ By pressing the + button, Web Service is selected from the options



➔ The name of the related vulnerability is written there and web service custom is selected as the type.



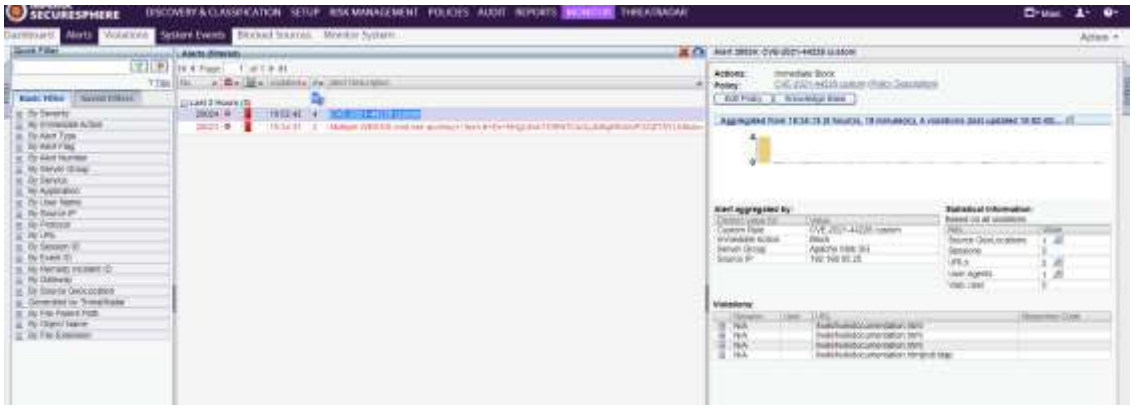
➔ In the panel that opens, signatures are selected as match criteria. And in the operations section, user defined signitures are selected, then the signatures that we have created before are taken from the left tab to the right (selected) tab. The action block, severity of the policy we have created should be high.



➔ The relevant services are selected in the Apply to section.

4. Monitor

If there is an attack to exploit this vulnerability, you can see that the CVE-2021-44228 policy is triggered in the Monitor>Alerts section.



Reference Links

https://nvd.nist.gov/vuln/detail/CVE-2021-44228

https://www.tenable.com/blog/cve-2021-44228-proof-of-concept-for-critical-apache-log4j-remote-code-execution-vulnerability