How to Mitigate the Log4j2 Vulnerabilities Using ASF

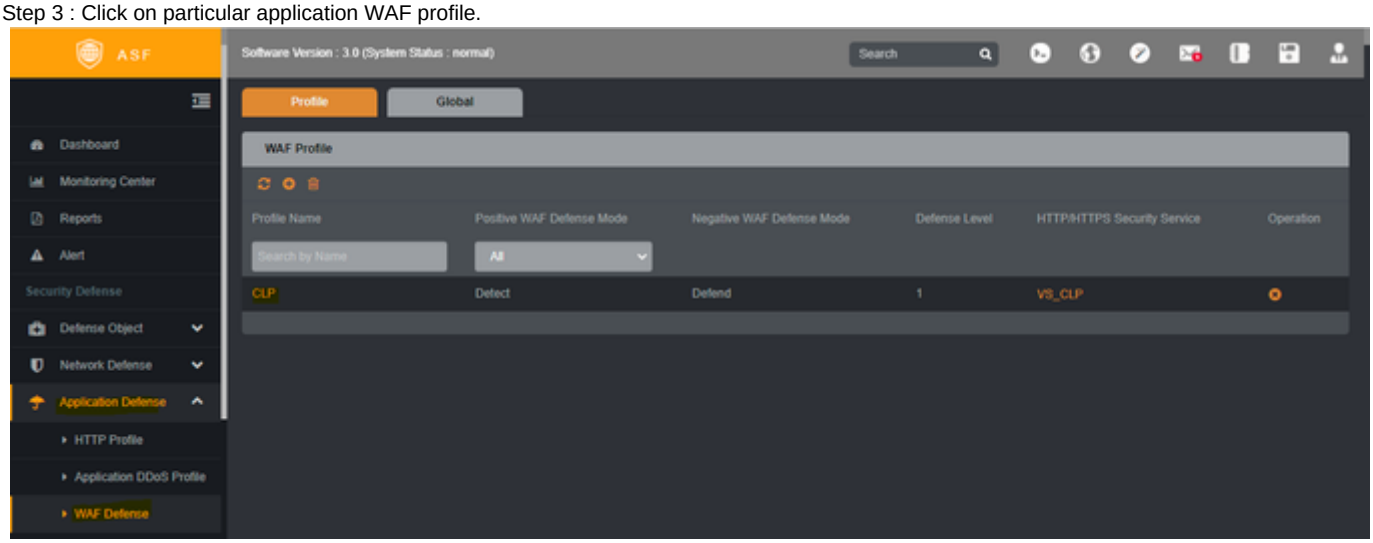
Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

The Array ASF will provide the protection from Log4j vulnerabilities CVE-2021-44228,CVE-2021-45046 and CVE-2021-45105. Please follow below steps to protect your application from log4j vulnerabilities.

Step 1 : Login into ASF webui

Step 2 : Click on “WAF defense” option under “Application Defense”.

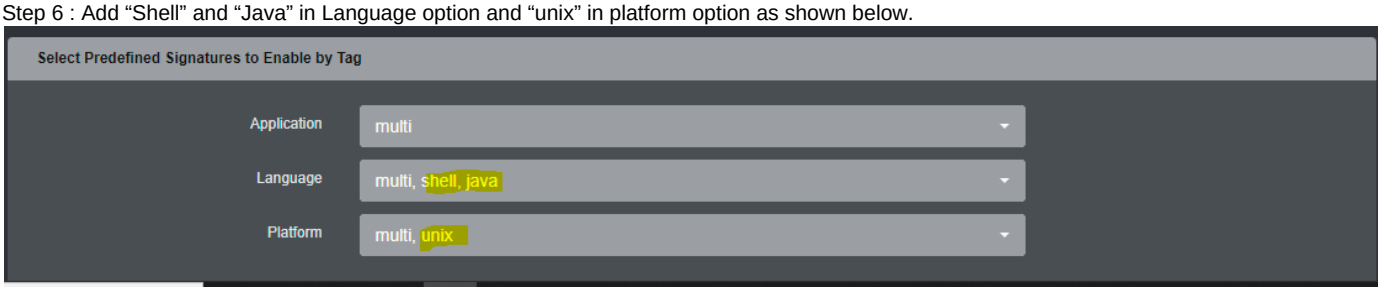
Step 3 : Click on particular application WAF profile.



Step 4 : Click on “negative waf” and then click on option “Signature-based defense” option.

Step 5 : Click on “General Settings” under “Signature-based defense” option

Step 6 : Add “Shell” and “Java” in Language option and “unix” in platform option as shown below.



Step 7 : Save the configuration.