

## CVE-2021-44228

### Explanation

This Security Warning addresses CVE-2021-44228, a remote code execution vulnerability in Apache Log4j. Attackers can be exploited remotely without authentication, meaning this vulnerability can be exploited over a network without requiring a username and password.

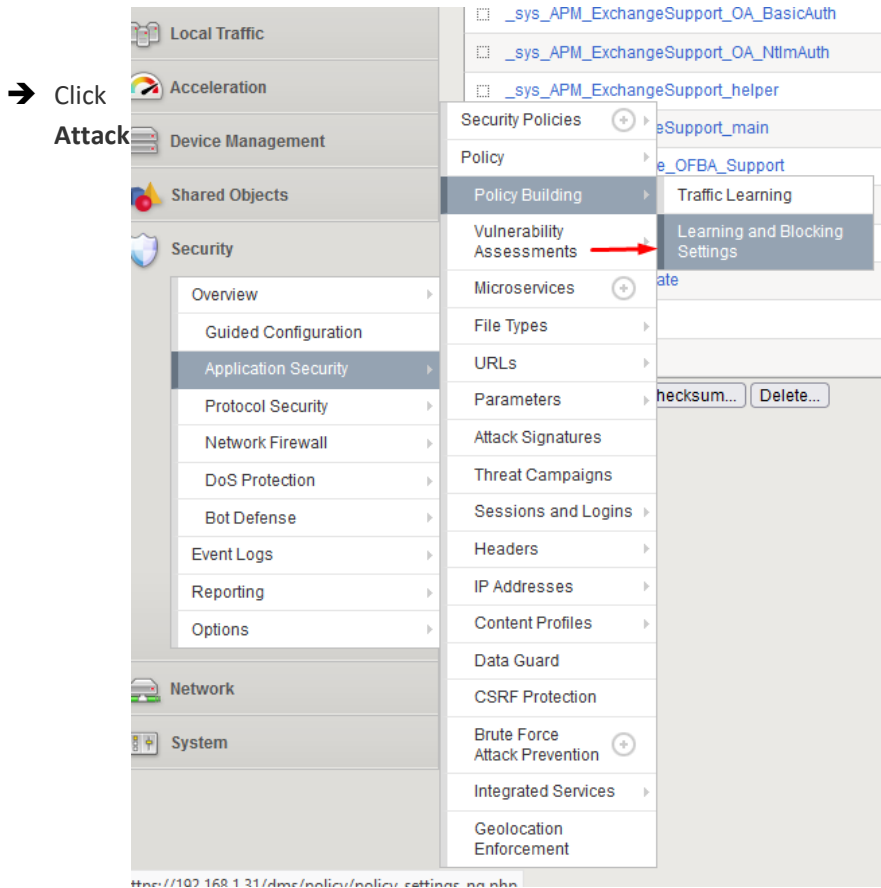
### Severity

Critical

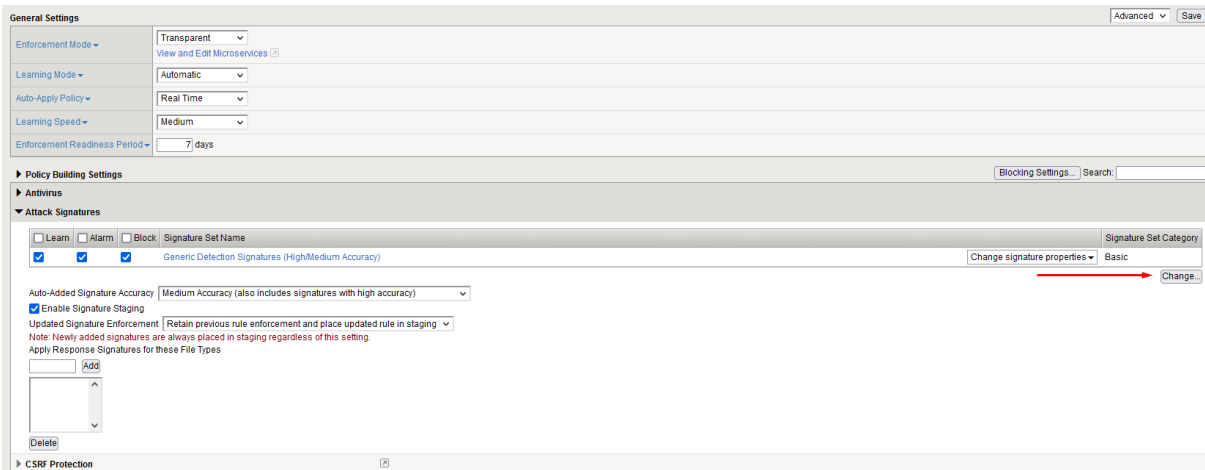
### Recommended Actions

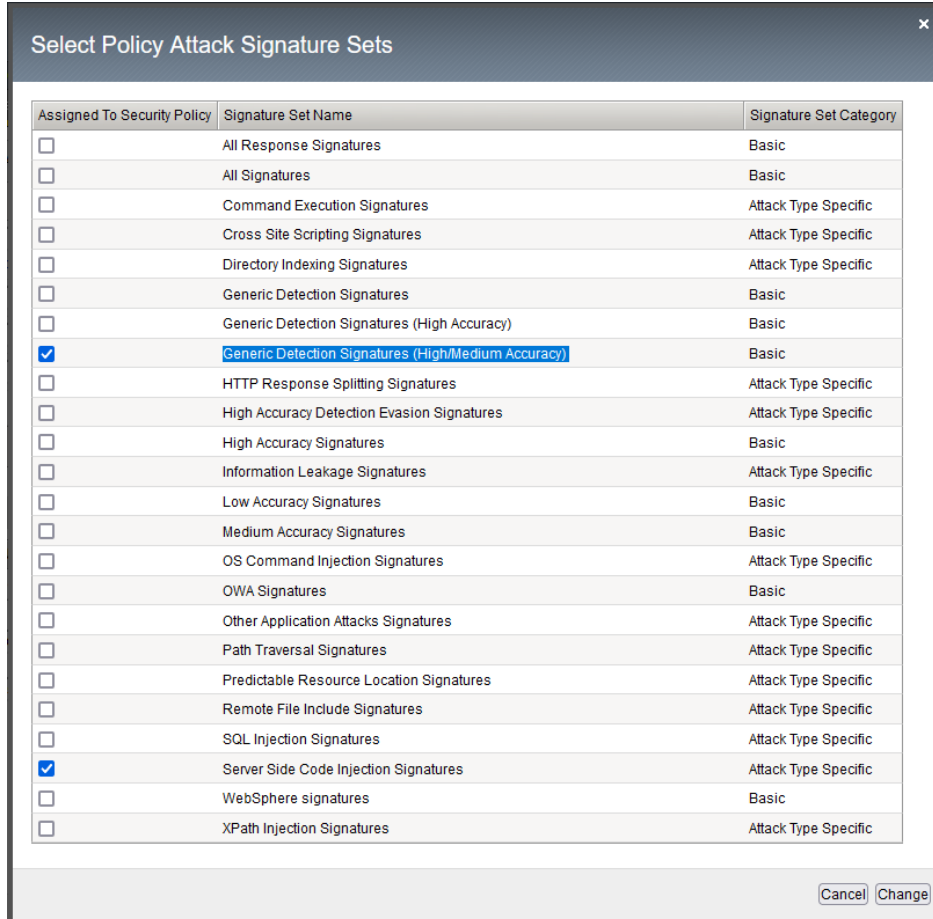
#### 1. WAF Policy

- Go to **Security>Application Security>Policy Building>Learning and Blocking Settings**. Make sure you have selected the appropriate security policy from the security policy list.



**Signatures.** Click **Change**. The Configuration utility displays a list of Attack Signature Sets in a new window.



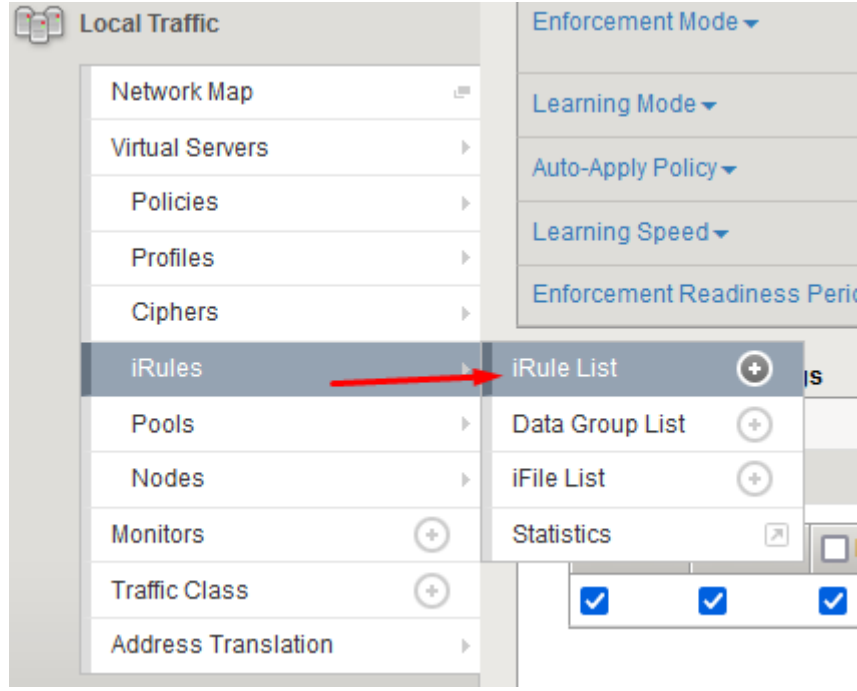


➔ Click **Save** and then click **Apply Policy**. Click **OK** to confirm applying the changes to the currently selected security policy.

| <input type="checkbox"/> Learn      | <input type="checkbox"/> Alarm      | <input type="checkbox"/> Block      | Signature Set Name                                  |
|-------------------------------------|-------------------------------------|-------------------------------------|---|
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Generic Detection Signatures (High/Medium Accuracy) |
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Server Side Code Injection Signatures               |

## 2.1-Rule

➔ To write CVE-2021-4428 specific irule, go to Local Traffic>iRule>iRule List menu. Click on Create button and a new iRule writing window opens.



- In the window that opens, a name is given to this irule and the specific generated code CVE-2021-4428 is entered in the definition part and the rule is saved by pressing the Finished button. (The written rule is given in the Appendix).

Properties

Name: Apache


```

5  if {[string tolower [URI::decode [HTTP::uri -normalized]] matches_regex {\$\{\}} {
6    log local0.debug "log4j_rce_detection drop on URI: [HTTP::uri -normalized]"
7    drop
8    event disable all
9    return
10 }
11
12 # Header - looks for ${j...} or ${${...}}
13 foreach name [HTTP::header names] {
14   if {[string tolower [HTTP::header values $name]] matches_regex {\$\{\{j|\$\{\}.\+\}\}} {
15     log local0.debug "log4j_rce_detection drop on header: [HTTP::header values $name]"
16     drop
17     event disable all
18     return
19   }
20 }
21
22 # Payload - looks for ${j...} or ${${...}}
23 if {[HTTP::method] eq "POST"}{
24   # Trigger collection for up to 1MB of data
25   if {[HTTP::header "Content-Length"] ne "" && [HTTP::header "Content-Length"] <= 1048576}{
26     set content_length [HTTP::header "Content-Length"]
27   } else {
28     set content_length 1048576
29   }
30   # Check if $content_length is not set to 0
31   if { $content_length > 0 } {
32     HTTP::collect $content_length
33   }
34 }
35 }
36 when HTTP_REQUEST_DATA priority 750 {
37   if {[string tolower [HTTP::payload]] matches_regex {\$\{\{j|\$\{\}.\+\}\}} {
38     log local0.debug "log4j_rce_detection drop on payload"
39     drop
40     event disable all
41   }
42 }

```

Definition

Wrap Text  
 Show Print Margin

Cancel Finished 

➔ Then enter the Virtual server where this rule will be applied. In the entered virtual server, there is the Manage button in the Irule tab under the Resources menu and click it.

Local Traffic » Virtual Servers : Virtual Server List » RGB\_VS

Properties Resources Security Statistics

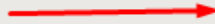
Load Balancing

Default Pool: RGB\_POOL

Default Persistence Profile: None

Fallback Persistence Profile: None

Update

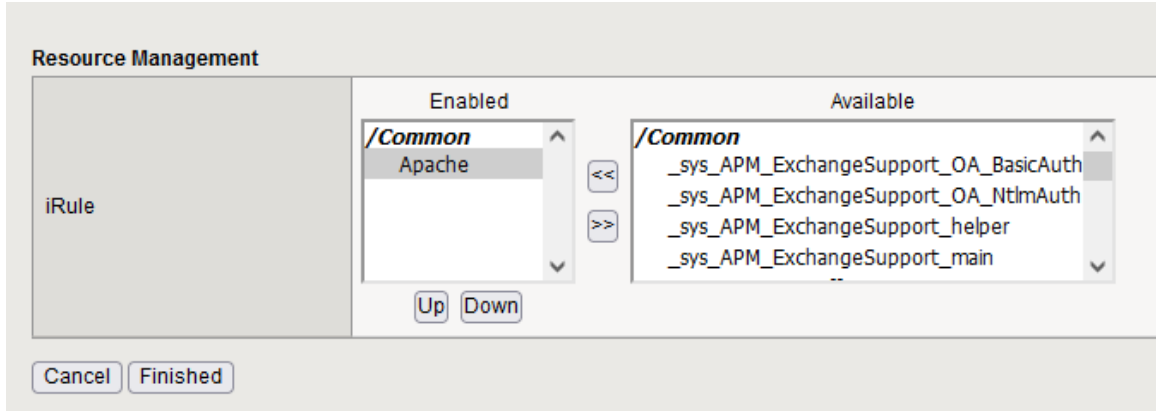
iRules  Manage...

Name

No records to display.

Manage

➔ In the menu that opens, select the I-Rule we created earlier and press finish.



## 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>

<https://support.f5.com/csp/article/K19026212>

# Appendix

```
when HTTP_REQUEST priority 750 {

# less aggressive regexp for those concerned about false positives "\${(env:[^:]+\S{[a-z]+})?(\${env:[^:]+\S{[a-z]+})?n.+}" (remove quotes)

# very aggressive regexp "\${.+?}" (remove quotes)

# URI – based on 200004474

if {[string tolower [URI::decode [HTTP::uri -normalized]]] matches_regex {\${}} {

log local0.debug "log4j_rce_detection drop on URI: [HTTP::uri -normalized]"

drop

event disable all

return

}

# Header – looks for ${j...} or ${${...}}

foreach name [HTTP::header names] {

if {[string tolower [HTTP::header values $name]] matches_regex {\${(j|\S{.})+.+?}} {

log local0.debug "log4j_rce_detection drop on header: [HTTP::header values $name]"

drop

event disable all

return

}

}

# Payload – looks for ${j...} or ${${...}}

if {[HTTP::method] eq "POST"}{

# Trigger collection for up to 1MB of data

if {[HTTP::header "Content-Length"] ne "" && [HTTP::header "Content-Length"] <= 1048576}{

set content_length [HTTP::header "Content-Length"]

} else {

set content_length 1048576

}

# Check if $content_length is not set to 0

if { $content_length > 0 } {

HTTP::collect $content_length

}

}

}

when HTTP_REQUEST_DATA priority 750 {

if {[string tolower [HTTP::payload]] matches_regex {\${(j|\S{.})+.+?}} {

log local0.debug "log4j_rce_detection drop on payload"

drop

event disable all

}

}
```