CVE-2021-44228

Description

Apache Log4j2 <=2.14.1 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.

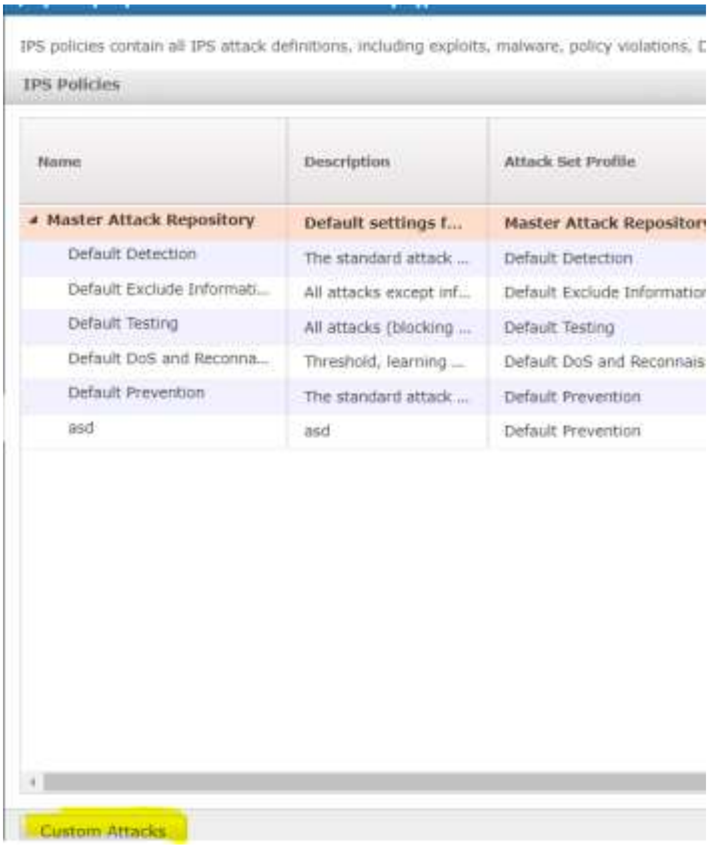
Severity

Critical

Action to be taken for Mcafee IPS

Emergency_UDS_2.zip

- ➔ The attached zip file must be downloaded
- ➔ Policy>Policy Types>IPS policies tabs should be followed
- ➔ Click on the Custom Attacks tab



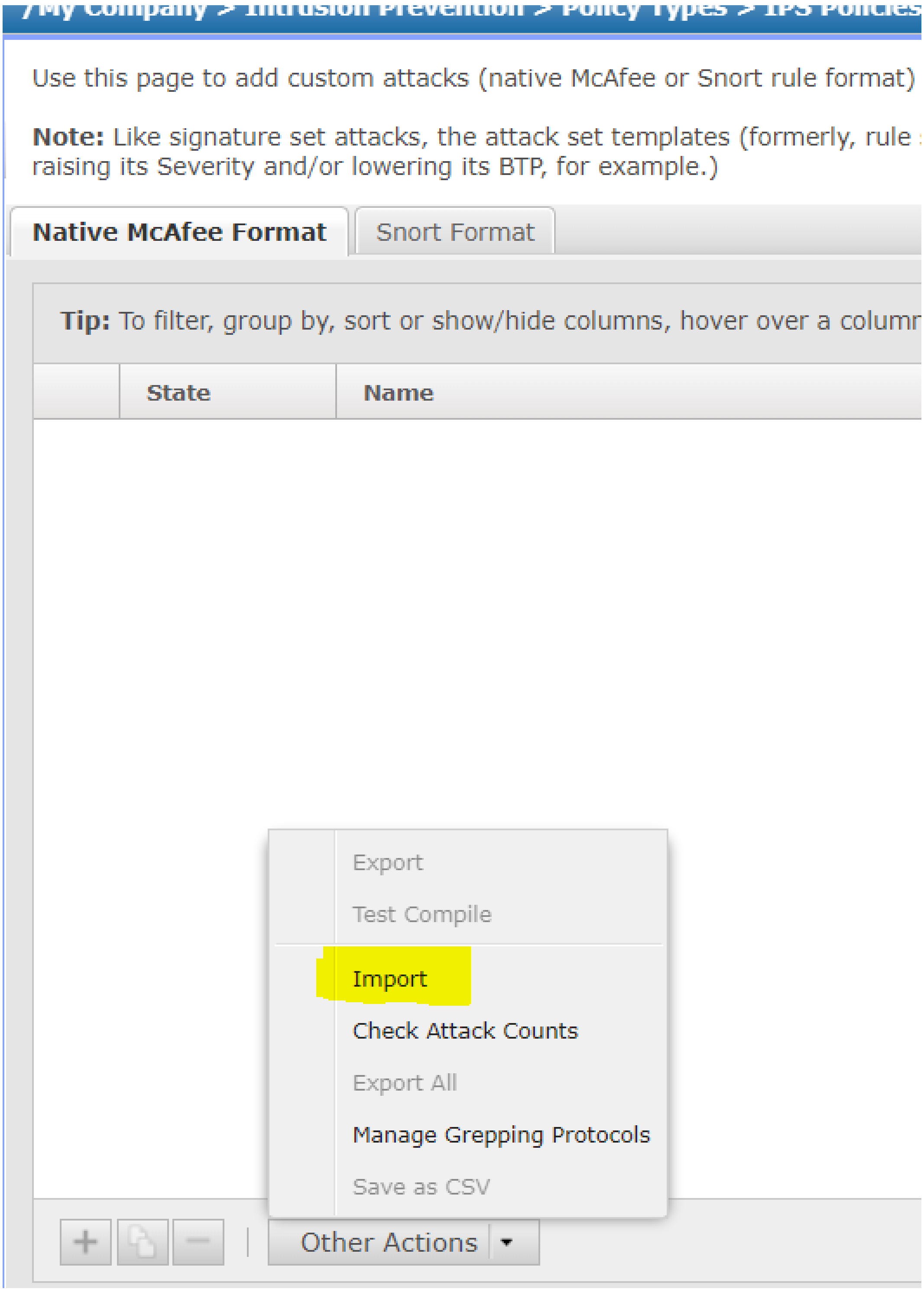
IPS policies contain all IPS attack definitions, including exploits, malware, policy violations, D

IPS Policies

Name	Description	Attack Set Profile
Master Attack Repository	Default settings f...	Master Attack Repository
Default Detection	The standard attack ...	Default Detection
Default Exclude Informati...	All attacks except inf...	Default Exclude Informatio
Default Testing	All attacks (blocking ...	Default Testing
Default DoS and Reconna...	Threshold, learning ...	Default DoS and Reconnais
Default Prevention	The standard attack ...	Default Prevention
asd	asd	Default Prevention

➔ Native Mcafee Format tab must be selected

➔ other actions> import tabs are followed.



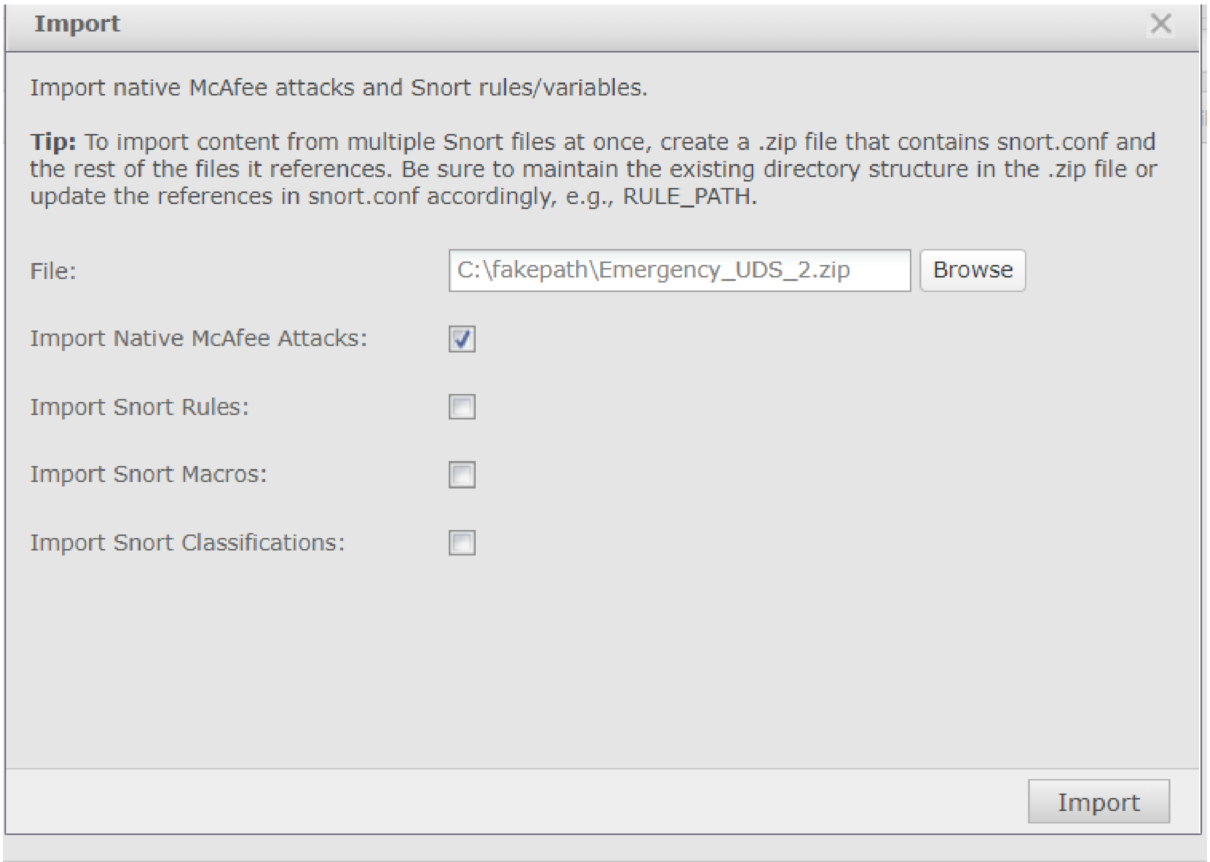
/My Company > Intrusion Prevention > Policy Types > IPS Policies

Use this page to add custom attacks (native McAfee or Snort rule format)

Note: Like signature set attacks, the attack set templates (formerly, rule raising its Severity and/or lowering its BTP, for example.)

Tip: To filter, group by, sort or show/hide columns, hover over a column

- ➔ We must add the attached file there in the tab that appears.
- ➔ Only Mcafee Native Attacks should be checked on this tab.



Import

Import native McAfee attacks and Snort rules/variables.

Tip: To import content from multiple Snort files at once, create a .zip file that contains snort.conf and the rest of the files it references. Be sure to maintain the existing directory structure in the .zip file or update the references in snort.conf accordingly, e.g., RULE_PATH.

File: C:\fakepath\Emergency_UDS_2.zip

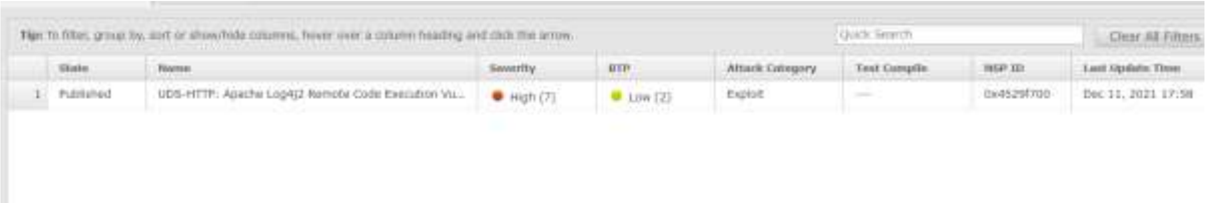
Import Native McAfee Attacks: ☑

Import Snort Rules: ☐

Import Snort Macros: ☐

Import Snort Classifications: ☐

- ➔ Click on Import to continue.
- ➔ After import, the custom signature list appears as follows.

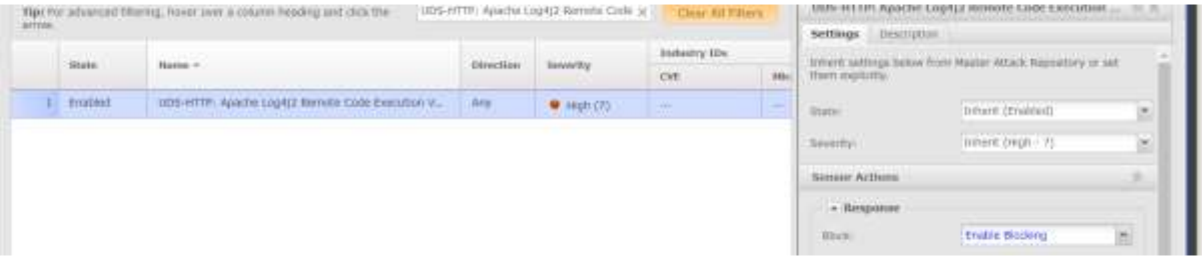


Tip: To filter, group by, sort or show/hide columns, hover over a column heading and click the arrow.

	State	Name	Severity	BTP	Attack Category	Test Compile	NSP ID	Last Update Time
1	Published	UDS-HTTP: Apache Log4j2 Remote Code Execution Vu...	● High (7)	● Low (2)	Exploit	—	0x4529f700	Dec 11, 2021 17:58

- ➔ By clicking Save, the signature you have imported is deployed to the policies.

- ➔ By following the Policy>Ips policies tab, the relevant signature in the policies used should be put in blocking mode.



Tip: For advanced filtering, hover over a column heading and click the arrow.

UDS-HTTP: Apache Log4j2 Remote Code

	State	Name	Direction	Severity	Industry IDs	
					CVE	Mi
1	Enabled	UDS-HTTP: Apache Log4j2 Remote Code Execution V...	Any	● High (7)	---	---

UDS-HTTP: Apache Log4j2 Remote Code Execution ...

Settings | Description

Inherit settings below from Master Attack Repository or set them explicitly.

State: Inherit (Enabled)

Severity: Inherit (High - 7)

Sensor Actions

Response

Block: Enable Blocking

➔ After the policy change, the sensor changes should be deployed.

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