CVE-2022-22963

Description

Spring4Shell is a bug in Spring Core, a popular application framework that allows software developers to quickly and easily develop Java applications with enterprise-level features. These applications can then be deployed on servers, such as Apache Tomcat, as stand-alone packages with all the required dependencies.

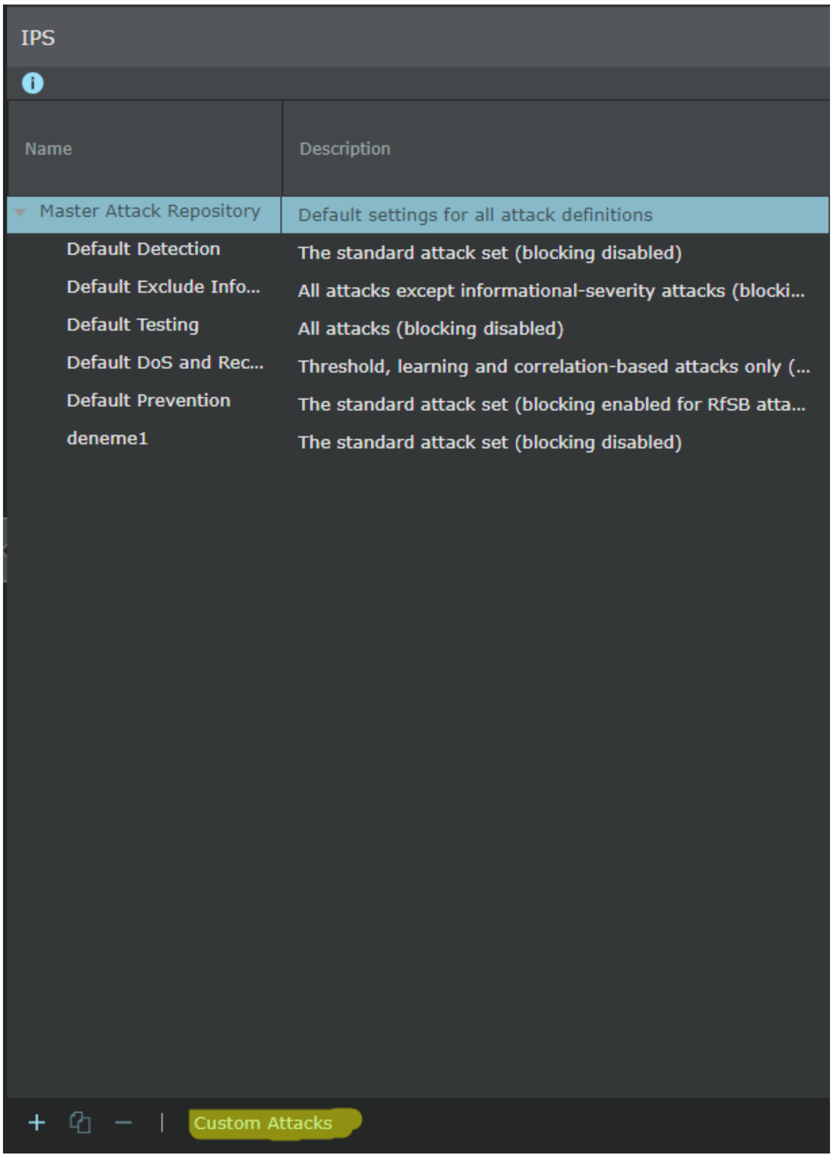
The bug allows an unauthenticated attacker to execute arbitrary code on a vulnerable system.

Severity

Critical

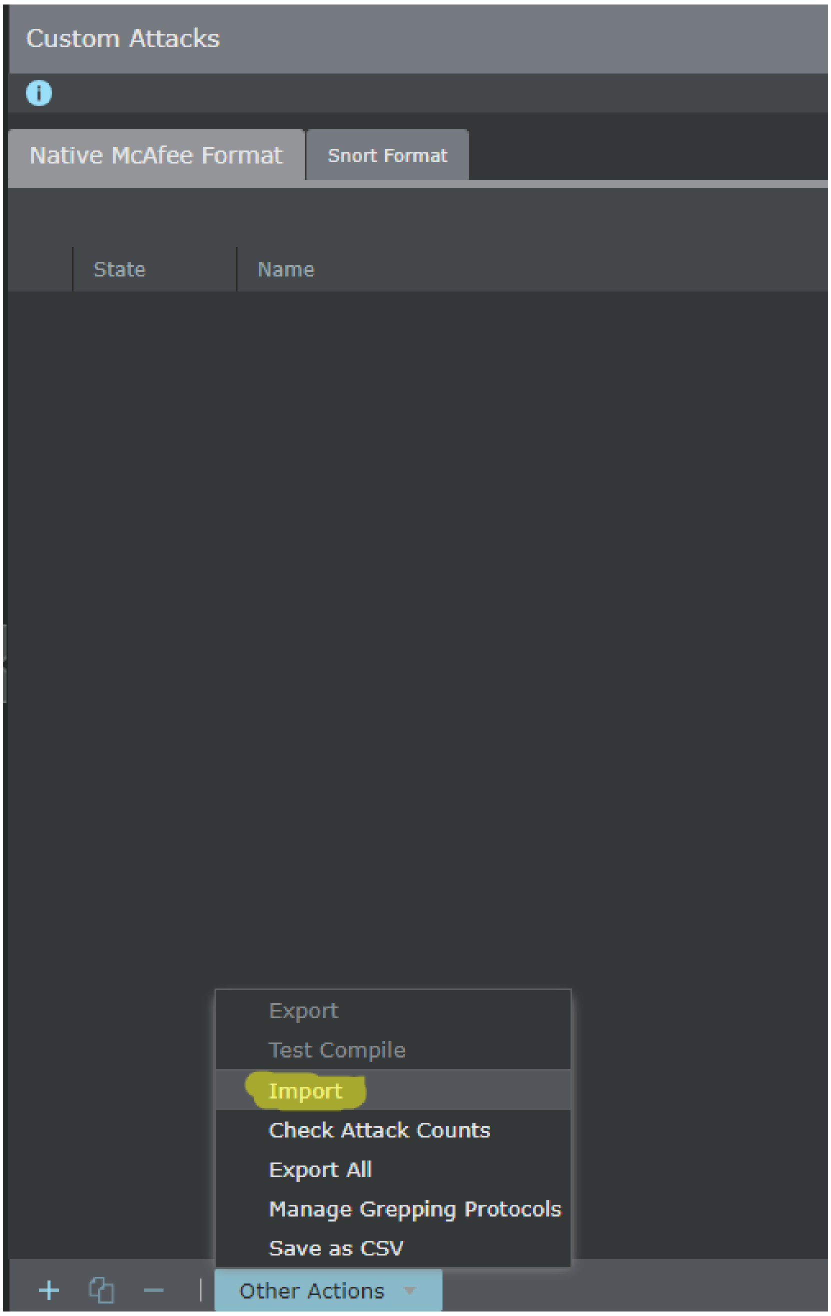
Action to be taken for Mcafee IPS

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



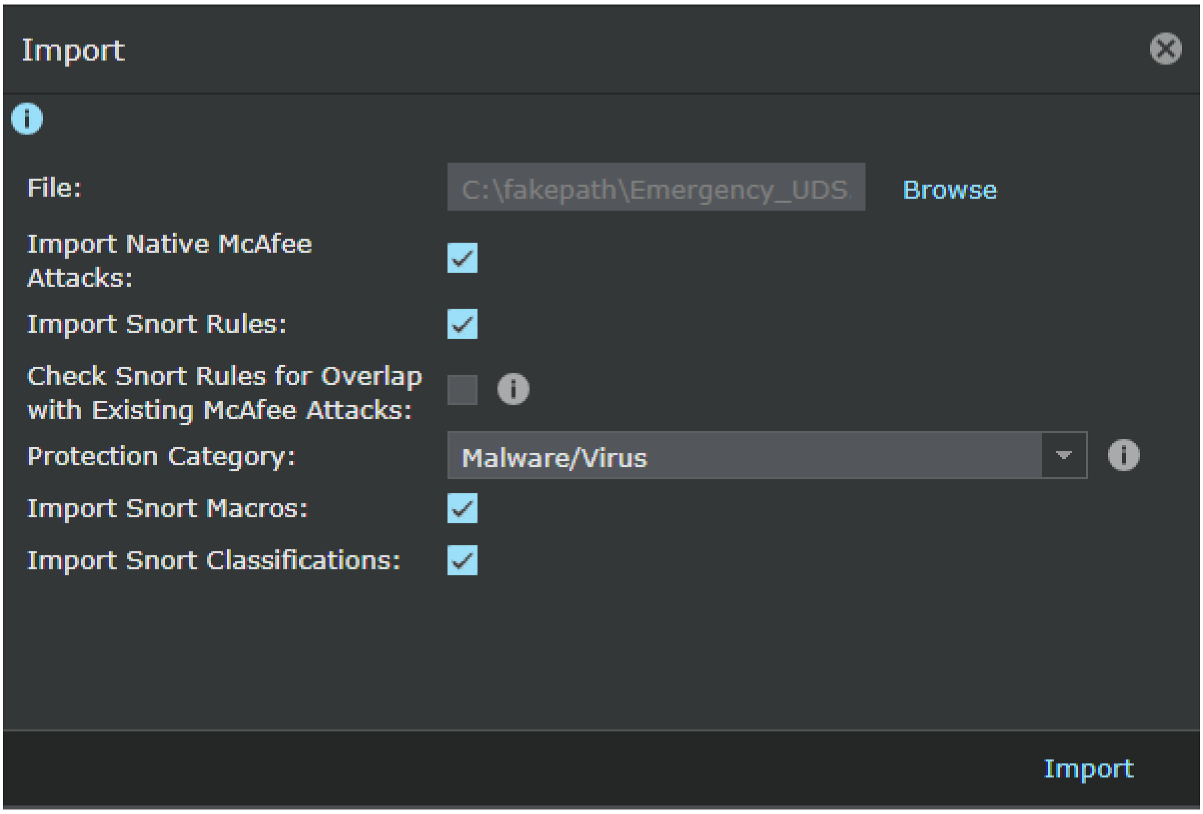
Name	Description
Master Attack Repository	Default settings for all attack definitions
Default Detection	The standard attack set (blocking disabled)
Default Exclude Info...	All attacks except informational-severity attacks (blocki...
Default Testing	All attacks (blocking disabled)
Default DoS and Rec...	Threshold, learning and correlation-based attacks only (...
Default Prevention	The standard attack set (blocking enabled for RfSB atta...
deneme1	The standard attack set (blocking disabled)

- ➔ Native Mcafee Format tab must be selected
- ➔ other actions> import tabs are followed.



➔ We must add the attached file there in the tab that appears.

➔ Only Mcafee Native Attacks should be checked on this tab.



Import

File: C:\fakepath\Emergency_UDS

Import Native McAfee Attacks: ☑

Import Snort Rules: ☑

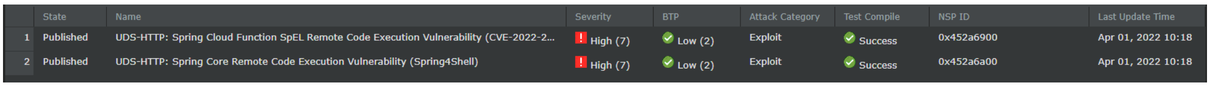
Check Snort Rules for Overlap with Existing McAfee Attacks: ☐

Protection Category: Malware/Virus

Import Snort Macros: ☑

Import Snort Classifications: ☑

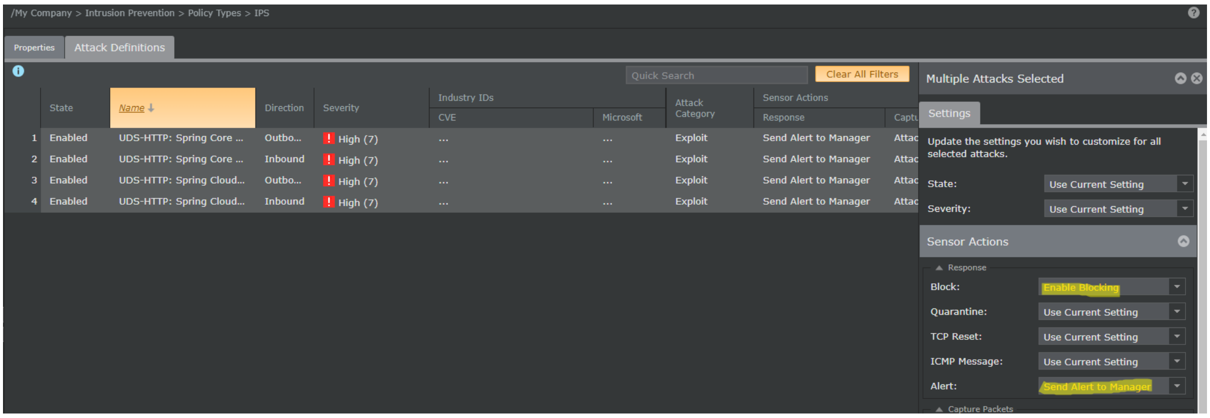
- ➔ Click on Import to continue.
- ➔ After import, the custom signature list appears as follows.



	State	Name	Severity	BTP	Attack Category	Test Compile	NSP ID	Last Update Time
1	Published	UDS-HTTP: Spring Cloud Function SpEL Remote Code Execution Vulnerability (CVE-2022-2...	! High (7)	✓ Low (2)	Exploit	✓ Success	0x452a6900	Apr 01, 2022 10:18
2	Published	UDS-HTTP: Spring Core Remote Code Execution Vulnerability (Spring4Shell)	! High (7)	✓ Low (2)	Exploit	✓ Success	0x452a6a00	Apr 01, 2022 10:18

- ➔ 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.



/My Company > Intrusion Prevention > Policy Types > IPS

Properties | Attack Definitions

Quick Search | Clear All Filters

	State	Name ↓	Direction	Severity	Industry IDs		Attack Category	Sensor Actions	
					CVE	Microsoft		Response	Captu
1	Enabled	UDS-HTTP: Spring Core ...	Outbo...	! High (7)	...	...	Exploit	Send Alert to Manager	Attac
2	Enabled	UDS-HTTP: Spring Core ...	Inbound	! High (7)	...	...	Exploit	Send Alert to Manager	Attac
3	Enabled	UDS-HTTP: Spring Cloud...	Outbo...	! High (7)	...	...	Exploit	Send Alert to Manager	Attac
4	Enabled	UDS-HTTP: Spring Cloud...	Inbound	! High (7)	...	...	Exploit	Send Alert to Manager	Attac

Multiple Attacks Selected

Settings

Update the settings you wish to customize for all selected attacks.

State: Use Current Setting

Severity: Use Current Setting

Sensor Actions

Response

Block: Enable Blocking

Quarantine: Use Current Setting

TCP Reset: Use Current Setting

ICMP Message: Use Current Setting

Alert: Send Alert to Manager

Capture Packets

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

Reference Links;

https://tanzu.vmware.com/security/cve-2022-22963

https://kc.mcafee.com/corporate/index?page=content&id=KB95447&locale=en_US