

CVE-2022-22963

Açıklama

Spring4Shell, yazılım geliştiricilerin Java uygulamalarını kurumsal düzeyde özelliklerle hızlı ve kolay bir şekilde geliştirmesine olanak tanıyan popüler bir uygulama çerçevesi olan Spring Core'daki bir hatadır. Bu uygulamalar daha sonra Apache Tomcat gibi sunucularda gerekli tüm bağımlılıklara sahip bağımsız paketler olarak dağıtılabilir.

Bug, kimliği doğrulanmamış bir saldırganın savunmasız bir sistemde rastgele kod yürütmesine izin verir.

Önem Derecesi

Kritik

Mcafee IPS için alınacak önlem

- Ekte bulunan zip dosyası indirilmeli
- Policy>Policy Types>IPS policies sekmeleri takip edilmeli
- Custom Attacks sekmesine tıklanmalı

IPS

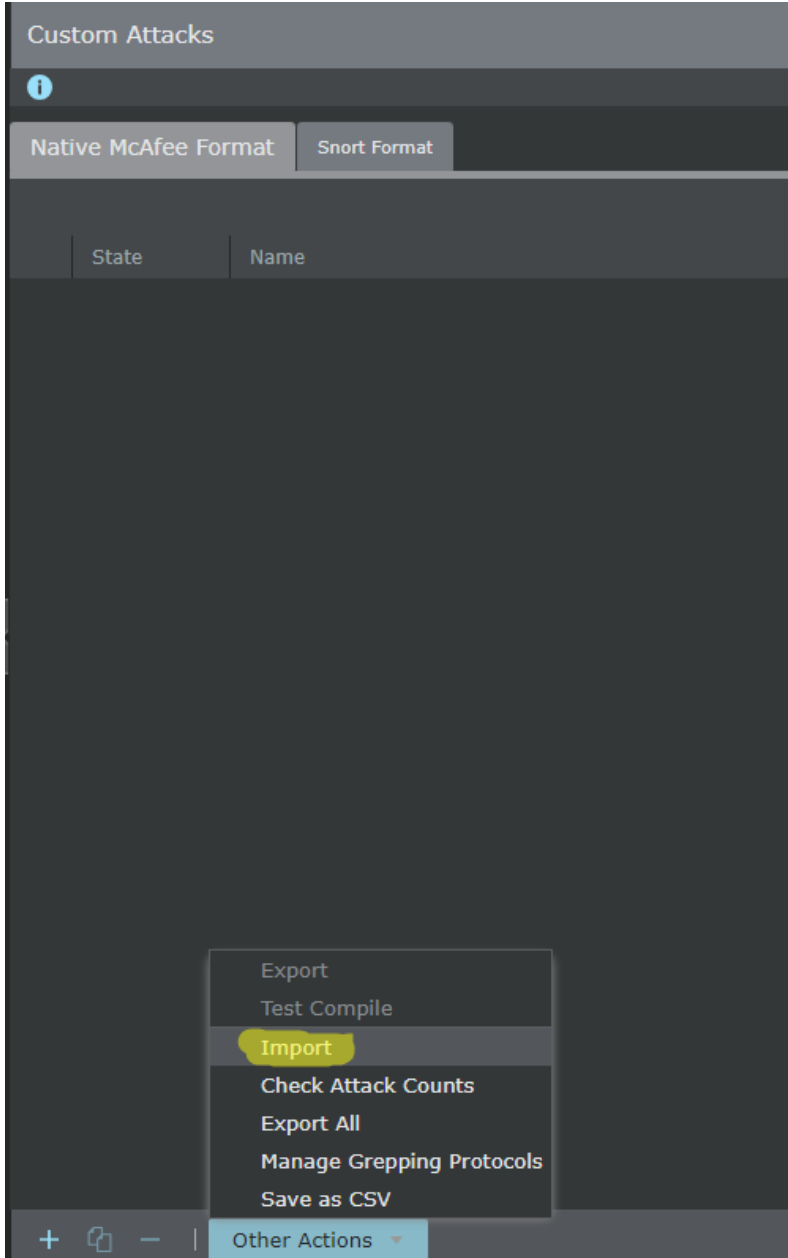
i

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)

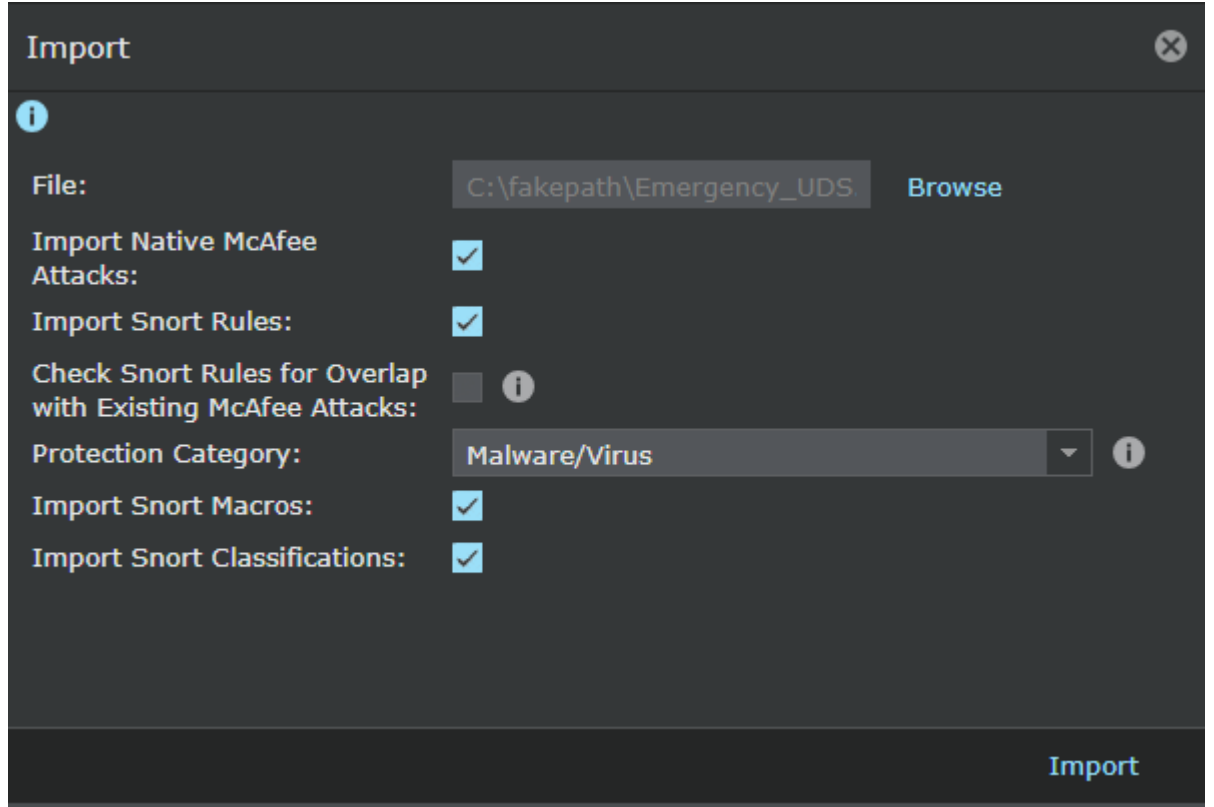
+ - | Custom Attacks

→ Native McAfee Format sekmesi Seçilmeli

→ Buradan other actions> import sekmeleri şeklinde devam edilmelidir.



- ➔ Emergency_UDS.ZIP dosyasını browse ederek eklemeliyiz.
- ➔ Bu sekmede yalnızca McAfee Native Attacks işaretli olmalıdır.



→ Import diyerek devam edilir.

→ Import sonrası custom imza listed aşağıdaki şekilde görülür.

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

→ Save diyerek import etmiş olduğunuz imzanın politikalara deploy edilmesi sağlanır.

→ Policy>Ips polices sekmesi takip edilerek, kullanılan politikalarda ilgili imza blocking moda alınmalıdır.

/My Company > Intrusion Prevention > Policy Types > IPS

Properties Attack Definitions

Quick Search Clear All Filters Multiple Attacks Selected

State	Name	Direction	Severity	Industry IDs	CVE	Microsoft	Attack Category	Sensor Actions	Response	Capture
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	

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

➔ Politika deęişiklięi sonrası sensore deęişiklikler deploy basılmalıdır.

Referans Baęlantıları

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

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