# 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.

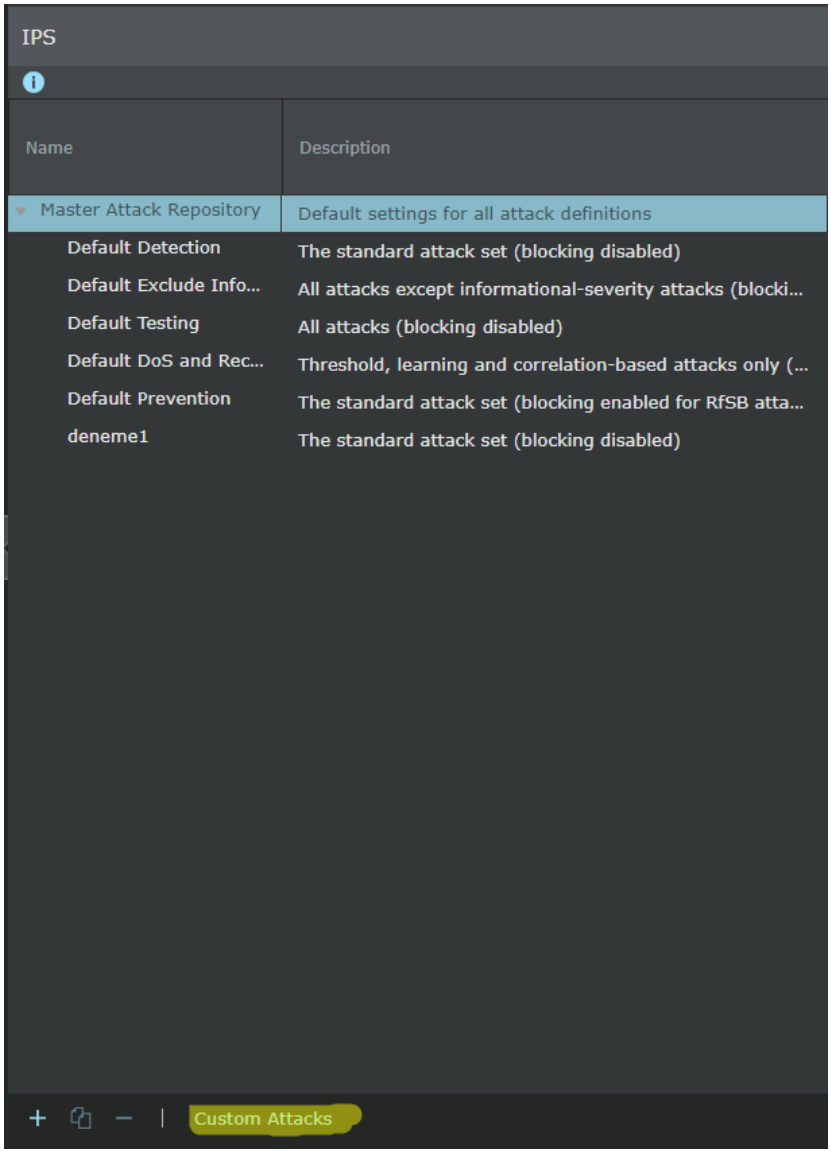
Bug, kimliği doğrulanmamış bir saldırganın savunmasız bir sistemde rastgele kod yürütmesine izin verir.

## Önem Derecesi

Kritik

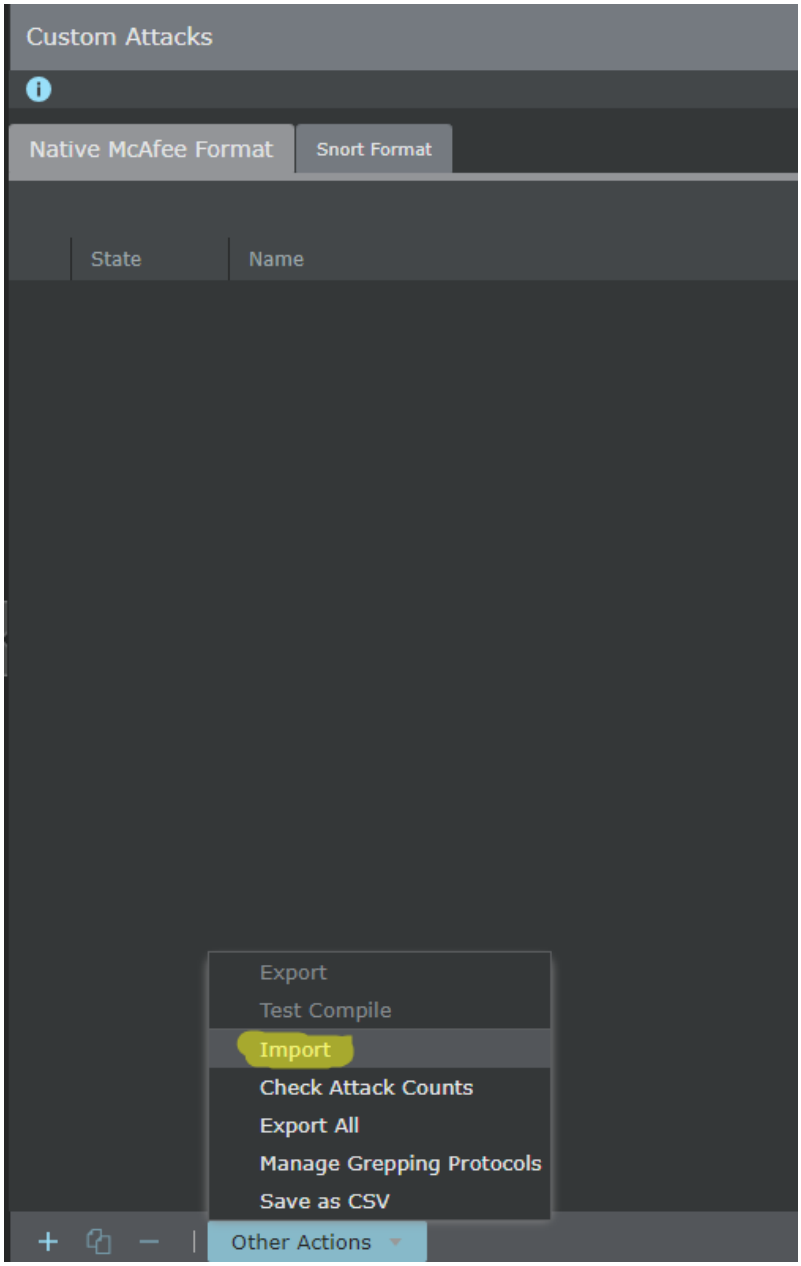
## Mcafee IPS için alınacak önlem

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

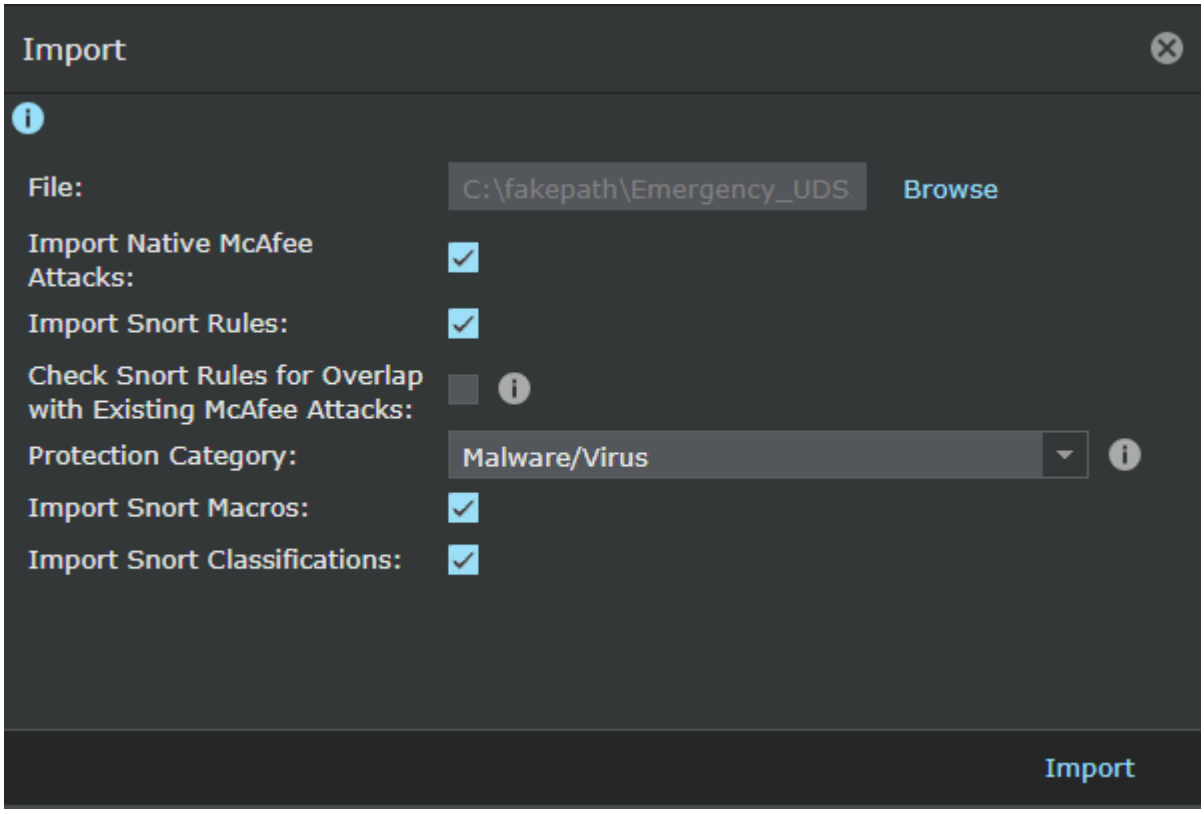



➔ Native Mcafee Format sekmesi Seçilmeli

➔ Buradan other actions> import sekmeleri şeklinde devam edilmelidir.

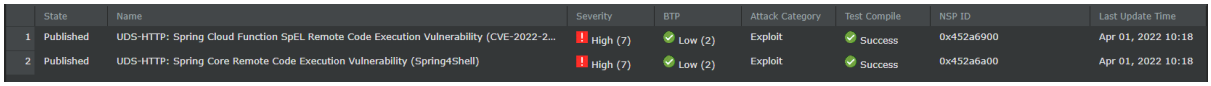



➔ Emergency_UDS.ZİP dosyasını browse ederek eklemeliyiz.
➔ Bu sekmede yalnızca Mcafee Native Attacks işaretli olmalıdır.




➔ Import diyerek devam edilir.

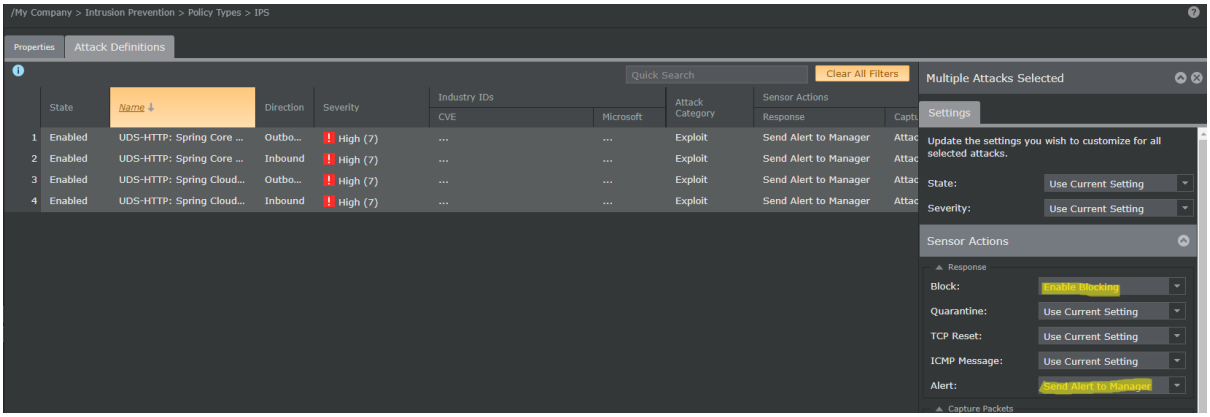
➔ Import sonrası custom imza listed aşağıdaki şekilde görülür.



| | 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.




➔ Politika değişikliği sonrası sensore değişiklikler deploy basılmalıdır.

## Referans Bağlantıları

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

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