CVE-2021-44228

Açıklama

Bu Güvenlik Uyarısı, Apache Log4j'deki bir uzaktan kod yürütme güvenlik açığı olan CVE-2021-44228'i ele alır. Saldırganlar kimlik doğrulama olmadan uzaktan kullanılabilir, yani bir kullanıcı adı ve parola gerekmeden bir ağ üzerinden bu zafiyet sömürülebilir.

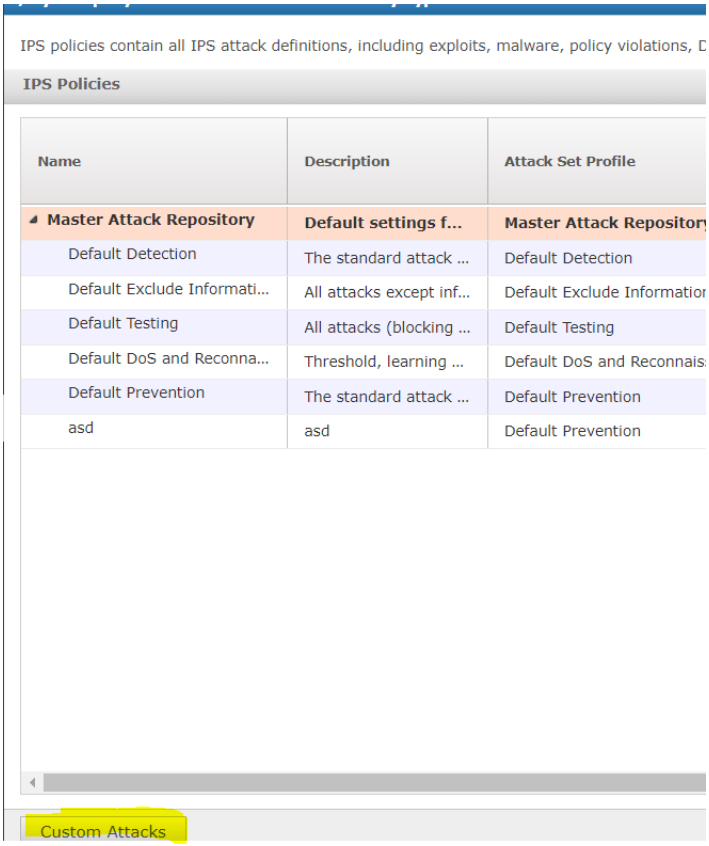
Önem Derecesi

Kritik

Mcafee IPS için alınacak önlem

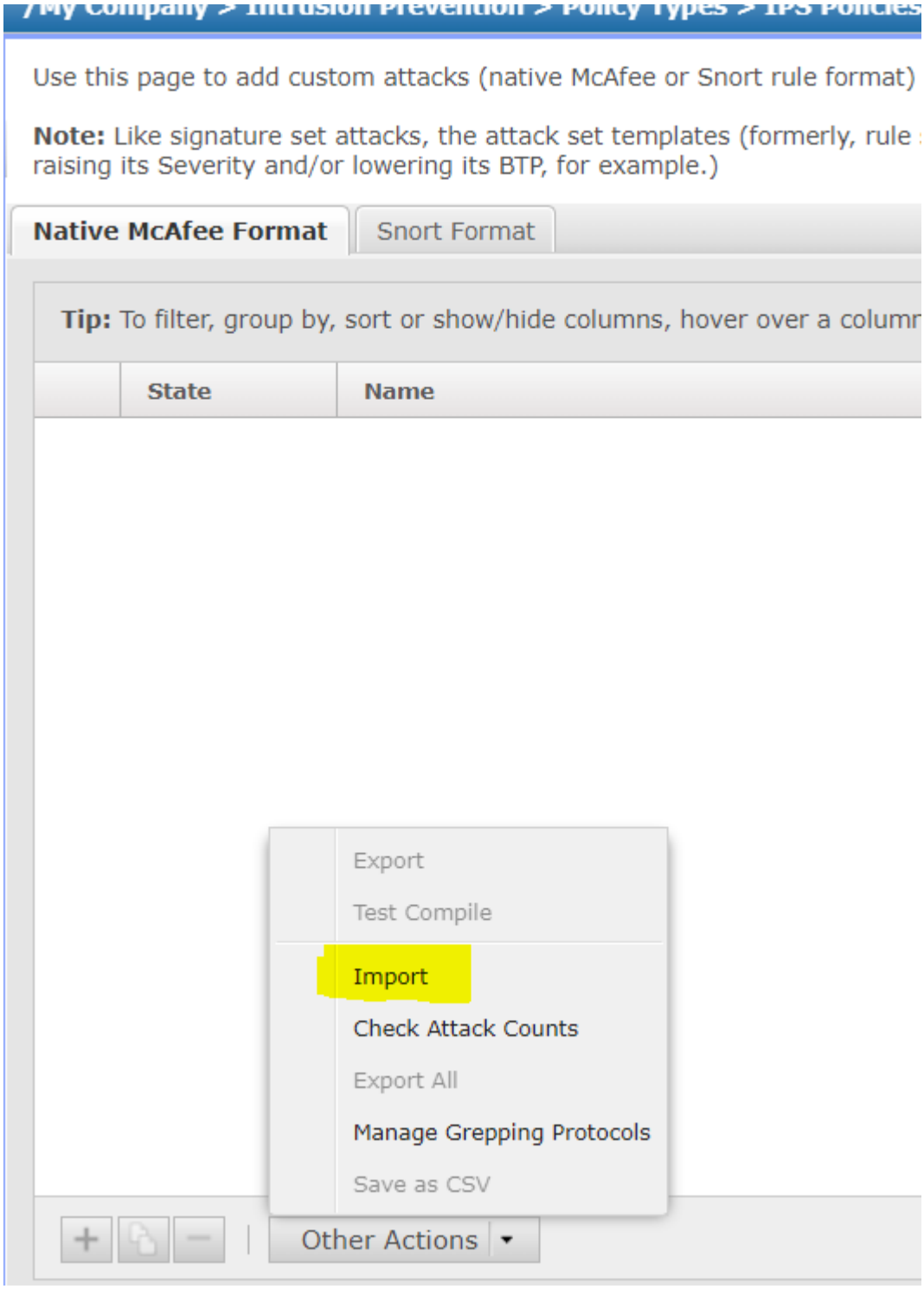
Emergency_UDS_2.zip

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

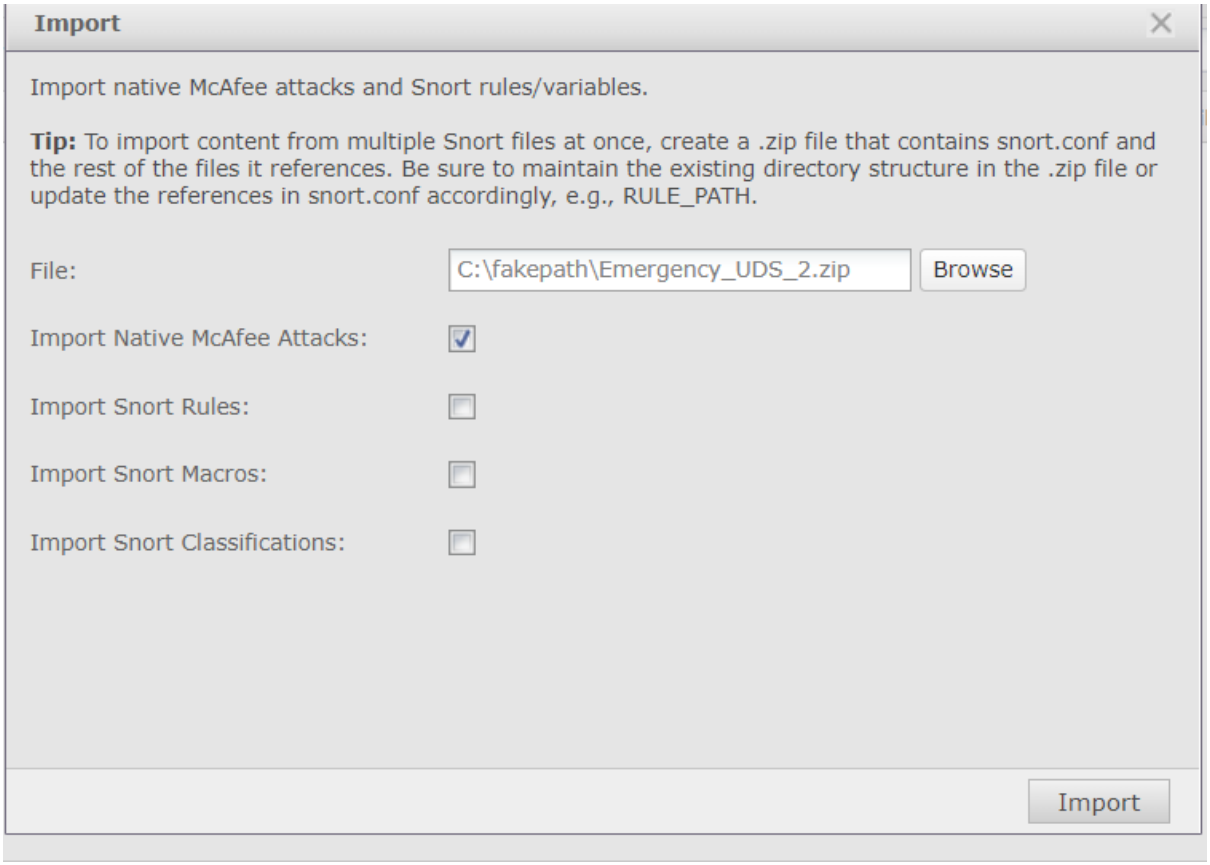


➔ Native Mcafee Format sekmesi Seçilmeli

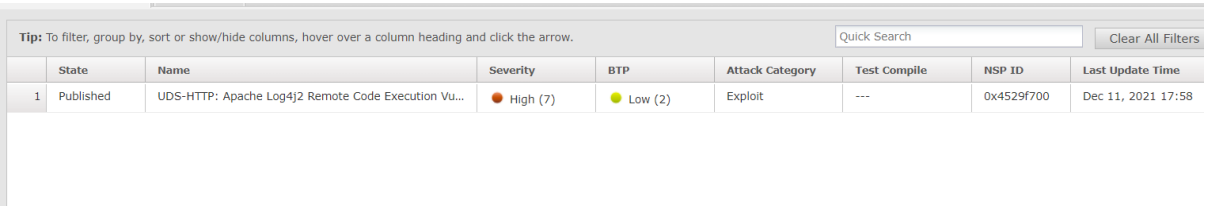
➔ Buradan other actions> import sekmeleri şeklinde devam edilmelidir.



➔ Ekteki dosyayı karşımıza çıkan sekmede oraya eklemeliyiz.
➔ Bu sekmede yalnızca Mcafee Native Attacks işaretli olmalıdır.

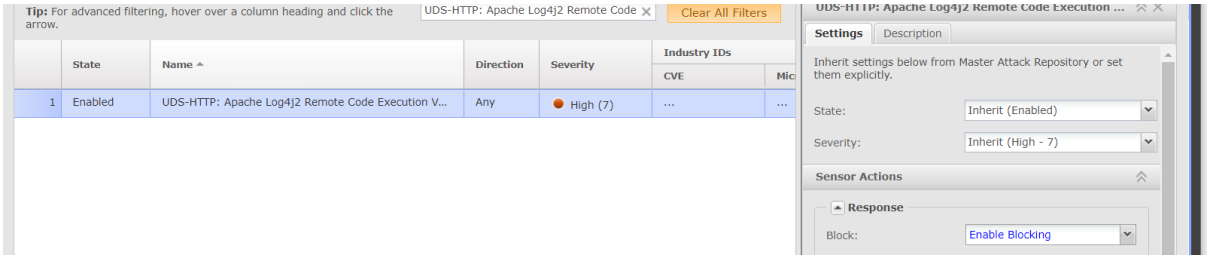


➔ Import diyerek devam edilir.
➔ Import sonrası custom imza listed aşağıdaki şekilde görülür.



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

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



Referans Bağlantıları

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