

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

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

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

Custom Attacks

HİZMETE ÖZEL / Sadece İç Kullanım

BARİKAT İÇ KULLANIM

- Native McAfee Format sekmesi Seçilmeli
- Buradan other actions> import sekmeleri şeklinde devam edilmelidir.

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.)

Native McAfee Format | Snort Format

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

State	Name
-------	------

Export

Test Compile

Import

Check Attack Counts

Export All

Manage Grepping Protocols

Save as CSV

+ | - | Other Actions ▾

- Ekteki dosyayı karşımıza çıkan sekmede oraya eklemeliyiz.
- Bu sekmede yalnızca McAfee Native Attacks işaretli olmalıdır.

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 Browse

Import Native McAfee Attacks:

Import Snort Rules:

Import Snort Macros:

Import Snort Classifications:

Import

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

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

Quick Search Clear All Filters

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

- Save diyerek import etmiş olduğunuz imzanın politikalara deploy edilmesi sağlanır.
- Policy>Ips polices sekmesi takip edilerek, kullanılan politikalarda ilgili imza blocking moda alınmalıdır.

HİZMETE ÖZEL / Sadece İç Kullanım

BARİKAT İÇ KULLANIM

Tip: For advanced filtering, hover over a column heading and click the arrow. UDS-HTTP: Apache Log4j2 Remote Code Execution x Clear All Filters

	State	Name ^	Direction	Severity	Industry IDs	
					CVE	Mic
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

Referans Baęlantıları

<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>

HİZMETE ÖZEL / Sadece İç Kullanım

BARİKAT İÇ KULLANIM