CVE-2021-44228

Explanation

This Security Alert addresses CVE-2021-44228, a remote code execution vulnerability in Apache Log4j. It is remotely exploitable without authentication, i.e., may be exploited over a network without the need for a username and password.

Severity

High

Precautions for Imperva WAF

1. Custom Dictionary creation

→ Setup>Signatures tabs are followed

→ Right click on the my dictionaries icon at the bottom of the left panel and select "create manual dictionary".



HİZMETE ÖZEL / Sadece İç Kullanım

BARİKAT İÇ KULLANIM

➔ In the panel that opens, the name of the related vulnerability is entered and web is selected as the type.

| Enter Name: | CVE2021-442 | 28 Apache Log4j | Vulnerability | | | | | 1 |
|--|-------------|-----------------|---------------|---------|----------|------------|-----------|---|
| Description: | | | | | | | | |
| Dictionary Type: Web Ostream Osgl | Oracle | MS SQL | Sybase | D82 | | SAP HANA | Informix | |
| | Teradata | Sybase IQ | MySQL | Netezza | Progress | PostgreSQL | Greenplum | |
| | ManaDB | Hive | HBase | Impala | MongoDB | Cassandra | | |

→ After clicking the Create option, the dictionary is created.

➔ In the next step, 4 signatures with the names "jndi:dns", "jndi:ldap", "jndi:rmi" and CVE-2021-44228-regexp, which are used in vulnerability payloads, are created in the dictionary we have previously created.

- When creating a signature here, signature part="jndi:ldap" for "jndi:ldap" and part="jndi:dns" for "jndi:dns" and part="jndi:rmi" for jndi:rmi should be written.
- For the CVE-2021-44228-regexp signature, it should be

part="\x24\x7b",rgxp="\x24\x7b.{0,30}j.{0,30}n.{0,30} d.{0,30}i.{0,30}\x3a.{1,150}"

- HTTP and https should be selected as Protocols.
- In Search signature in section, Parameters, Request body, URL, Headers, Non-Normalized URL should be selected.

| Constant of Manager | 0.00 | | | | |
|---|---|-----------------------|--|-------------|---|
| Signature Name. | CVE-2021-44228-regexp | Te in 101 in 101 | 10 100 4 10 100 10 100 -000 -00 | is said | |
| Signature | DUI- 423 KID 1040- 423 6 | RUR for sold for sold | to sold to solr to sol 424 | ((), (out)) | |
| | Predefined | | Selected. | _ | |
| Protocols: | | * * | ntip | ţ. | |
| | Predefined | | Selected: | | |
| Search Signature In: | Urls And Parameters | | Non Normalized Un Parameters | ÷. | |
| | | | Create | Cancel | |
| | | | | | 1 |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| d Signature | | | | | x |
| Id Signature | [indi:ldap | | | | |
| Id Signature gnature Name: | jndi:ldap part="indi:ldap" | | | | × |
| Id Signature jnature Name: jnature: | jndi:ldap part="indi:ldap" | | | | × |
| Id Signature gnature Name: gnature: | jndi:Idap part="indi.Idap" | | | | |
| I d Signature gnature Name: gnature: | jndi:ldap part="indi:ldap" Predefined | | Selected: | | |
| Id Signature gnature Name: gnature: ptocols: | jndi:ldap part="indi:ldap" Predefined | | Selected: | | |
| Id Signature gnature Name: gnature: ptocols: | jndi:ldap part="indi:ldap" Predefined | | Selected: | | |
| Id Signature gnature Name: gnature: ptocols: | jndi:ldap patt="jndi.ldap" Predefined | | Selected: http https | | |
| Id Signature gnature Name: gnature: ptocols: | jndi:ldap patt="indi:ldap" Predefined Predefined Response Content | | Selected: http https Selected: Headers | | |
| Id Signature gnature Name: gnature: ptocols: arch Signature In: | jndi:ldap patt="indi:ldap" Predefined Predefined Response Content Urls And Parameters | | Selected: http https Selected: Headers Non Normalized | Un | |
| Id Signature gnature Name: gnature: otocols: arch Signature In: | jndi:ldap patt="indi:ldap" Predefined Predefined Response Content Urls And Parameters | | Selected: http https Selected: Headers Non Normalized Parameters | | |

→ A signature is created with the Create button

→ The final image should be as follows.

| CVE-2021-44228 Lop4J Vulnerability - Manual, Web | ** | CVE-2021-44228- | фхадаг |
|---|--|-------------------------------------|--|
| Description: | | Bignature Name Signature Pattern | CVE 2021 44228-regexp part="x24x7b" rgxp="x24 (0.30)n (0.30)d (0.30) {0.30 |
| Name Patient CVE 2021-4226-regime pan="x22xx7b" rgsp="x22xx7b (0.30); (0. | Protocol http:rttps http:rttps http:rttps http:rttps http:rttps | Protocols | Predefined |
| | | Search Signature In | Predefined Response Cor A Urts And Para T |

HİZMETE ÖZEL / Sadece iç Kullanım BARİKAT İÇ KULLANIM

- 2. Web Service Policy creation
- → Policies>Security tabs are followed
- \rightarrow By pressing the + button, web service is selected from the options.

| Ç | | RY & CLASSIFICATION SETUP RISK MA | NAGEMEI | NT POLICIES A | |
|-------|----------------------------------|-----------------------------------|-----------------|-------------------|--|
| S | ecurity Audit Data Enrichment Sy | stem Events Action Sets | | | |
| | Basic Filter Saved Filters | Policies | | 🛧 🗯 Policy nam | |
| | By ADC Keywords | Policy | Туре | Web Service | |
| _ | 🗄 Ву Туре | - LITTD/4 v Protocol Volidation | Web Application | | |
| Ite | By Level | E H TP/1.X Protocol validation | | DB Service | |
| E | By Server Group | DenemeCustom sigpolicy | HITP/1. | DB Application | |
| | By Service | DenemeCustom sigpolicy2 | HTTP/1. | Network | |
| | By Application | HTTP/1.x Protocol Policy H | | Snippet Injection | |
| 8 | Default Policies | Soliniection Plicy HTTP/1 | | HDFS Service | |
| olici | Policy Origin | | | z/OS DB Service c | |
| ۵. | | DB Protocol Validation | | - Ciar | |
| | | SQL Protocol Policy | DB Proto | ocol 🛛 🖉 🗸 Sigi | |
| | | test | DB Proto | ocol Available | |

➔ In the opened tab, the name of the related vulnerability is written and http protocol signatures is selected as the type.



➔ By pressing the + button in the Policy Rules tab, the dictionary we created in the 1st step is selected. The final state should be the same as the screenshot. So Severity should be no alert and action should be none.

| Dictionary Name | 🕂 📕 Enabled | Bevecty. | | Action | | Followed Action | |
|--|-------------|----------|---|--------|---|-----------------|---|
| III CVE-2021-44228 Abache Loo4i Wanerabaty | | No Alert | * | None | ~ | 1 | ~ |

HİZMETE ÖZEL / Sadece iç Kullanım BARİKAT İÇ KULLANIM → After saving the changes, the policy is assigned to the relevant services from the apply to tab.

| olicy Rules | Apply To | Advanced | Activity Log |
|-------------|---------------------------|----------|--------------|
| - 🔁 🖻 All | | | |
| 🖻 🚠 🕑 Ap | ache | | |
| िक्के 🖂 De | f <mark>ault S</mark> ite | | |
| 🗄 💑 🗹 Su | perVeda | | |
| 🕀 🔂 🖂 mis | sc2012 | | |
| | | | |
| | | | |
| | | | |

3. Creating a Web Service custom policy

→ Policies>Security tabs are followed

→ By pressing the + button, Web Service is selected from the options

| | SPHERE DI | SCOVER | & CLASSIFICATION SETUP RISK MANAGEMEI | NT POLICIES | AUDIT |
|---|---|---------|---|--------------------------------|----------------|
| Basic Filter | t Data Enrichme Saved Filters | nt Syst | em Events Action Sets Policies | 🛨 💢 Policy ni | ime: CVE |
| By ADC Key | words | 12 | A Page 3 of 6 > >1 Policy | Web Service Web Application | riteria |
| By Level By Server G By Service | By Level By Server Group By Service | | Web Service Custom | DB Service DB Application | Action |
| By Application Default Police | on des | | CVE-2018-20062 ThinkPHP S x Hemote Code Execution CVE-2018-20062 ThinkPHP Remote Code Execution | Snippet Injection | e: Criteria |
| Policy Origin | 1 | 2 | CVE-2016-20243: Apache Fineract Cleantext URL Crei CVE-2018-8823: PrestaShop Responsive Mega Menu- | 2/OS DB Service | sie Matc |
| | | | CVE-2019-10392 Git Client Plugin for Jenkins git is-ren | note E + A | pplication |

➔ The name of the related vulnerability is written there and web service custom is selected as the type.

| ie CVE-2021-4422 | 8 Log4J Vulnerability | |
|-------------------------|---------------------------|--------|
| From Scratch | | |
| Туре: | Web Service Custom | ~ |
| \bigcirc Use existing | | |
| -CVE-2021- | 44228 Log4J Vulnerability | ~ |
| | Create | Cancel |

→ In the panel that opens, signatures are selected as match criteria. And in the operations section, user defined signitures are selected, then the signatures that we have created before are taken from the left tab to the right (selected) tab. The action block, severity of the policy we have created should be high.

| Policy Configuratio | e: | Signatures is at least one of (ind: dna. indi: | m Fall Description | | |
|---------------------|-----------------------|--|---------------------------------------|-------|---|
| Action: | Block | ~ | Severity: | High | |
| ollowed Action | qradar | ~ | Enabled | M Yes | |
| lert Name: | Custom Violation | | One Alert Per Session | 0 🖬 | |
| Match Criteria | | | | | |
| Signatures | | | | | |
| Operation | | At least one | | | × |
| User Defined Sign | atures | ~ | Selected: | | |
| admin | | | proti dhis proti idap proti imi | | |
| Available Match 0 | Criteria | | aus | | |
| 🛛 🛧 Account Taki | eover Protection Resi | ifts | | | |
| + Application L | Jser | | | | |
| + Authenticate | d Session | | | | |
| Authenticatic | in Result | | | | |
| | | | | | |
| il + Authenticatio | an URL | | | | |

HİZMETE ÖZEL / Sadece İç Kullanım BARİKAT İÇ KULLANIM → The relevant services are selected in the Apply to section.

| Policy name: CVE- | 2021-44228 c | ustom | | |
|-------------------|-------------------|----------|--------------|--|
| Match Criteria | Apply To | Advanced | Activity Log | |
| 🗄 🗁 🖃 All | | | | |
| E B Apac | he | | | |
| | uit Site rVeda | | | |
| 🕀 🚓 🖂 misc | 2012 | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

4. Monitor

If there is an attack to exploit this vulnerability, you can see that the CVE-2021-44228 policy is triggered in the Monitor>Alerts section.



HİZMETE ÖZEL / Sadece İç Kullanım BARİKAT İÇ KULLANIM

Reference Links

https://nvd.nist.gov/vuln/detail/CVE-2021-44228

https://www.tenable.com/blog/cve-2021-44228-proof-of-concept-for-critical-apache-log4j-remotecode-execution-vulnerability

> HİZMETE ÖZEL / Sadece İç Kullanım BARİKAT İÇ KULLANIM