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

Imperva WAF için alınacak önlem

1. Custom Dictionary oluşturulması

→ Setup>Signitures sekmeleri takip edilir

➔ Sol panelde en altta bulunan my dictionaries sekmesine sağ tık yapılarak "create manuel dictionary" seçilir.



HİZMETE ÖZEL / Sadece İç Kullanım

BARİKAT İÇ KULLANIM

→ Açılan panelde ilgili zafiyetin ismi girilir ve type olarak web seçilir.

E2021-4422	8 Apache Log4j	Vulnerability					
Oracle	MS SQI	Sybase	DB2	IMS	SAP HANA	Informix	
Teradata	Sybase IO	MySOL	Netezza	Progress		Greenplum	
MariaDB	Hive	HBase			Cassandra	Greenplan	
	Oracle Teradata MariaDB	Oracle MS SQL Teradata Sybase IQ MariaDB Hive	Oracle MS SQL Sybase Teradata Sybase IQ MySQL MariaDB Hive HBase	Oracle MS SQL Sybase DB2 Teradata Sybase IQ MySQL Netezza MariaDB Hive HBase Impala	Oracle MS SQL Sybase DB2 IMS Teradata Sybase IQ MySQL Netezza Progress MariaDB Hive HBase Impala MongoDB	Oracle MS SQL Sybase DB2 IMS SAP HANA Teradata Sybase IQ MySQL Netezza Progress PostgreSQL MariaDB Hive HBase Impala MongoDB Cassandra	Oracle MS SQL Sybase DB2 IMS SAP HANA Informix Teradata Sybase IQ MySQL Netezza Progress PostgreSQL Greenplum MariaDB Hive HBase Impala MongoDB Cassandra

- → Create seçeneğine basıldıktan sonra dictionary oluşturulur.
- → Sonraki aşamada oluşturmuş olduğumuz dictionary içerisine zafiyet payloadlarında kullanılan "jndi:dns", "jndi:ldap", "jndi:rmi" ve CVE-2021-44228-regexp ismiyle 4 adet imza oluşturulur.
 - Burada imza oluştururken "jndi:ldap" için signature part="jndi:ldap" şeklinde "jndi:dns" için part="jndi:dns" jndi:rmi için part="jndi:dns" şeklinde imza tanımı yazılmalıdır
 - CVE-2021-44228-regexp imzası için ise part="\x24\x7b",rgxp="\x24\x7b.{0,30}j.{0,30}n.{0,30} }d.{0,30}i.{0,30}\x3a.{1,150}" şeklinde regex yazılmalıdır
 - Protocols olarak http ve https seçilmelidir.
 - Search signiture in kısmında ise Parameters, Request body, URL, Headers, Non-Normalized URL şeçili olmalıdır.

Signature Name:	CVE-2021-44228-regexp
Signature:	part="\x24\x7b".rgxp="\x24\x7b.{0,30}j.{0,30}g.{0,30}g.{0,30}i.{0,30}\x3a.{1,150}"
	Predefined Selected:
Protocols:	https
	Predefined Selected:
Search Signature In	n: Urls And Parameters
	Create Cancel
Signature	×
I Signature	Indikton
Signature ature Name:	jndi:ldap
I Signature lature Name: lature:	jndi:Idap part="jndiJdap"
I Signature lature Name: lature:	jndi:ldap part="indi:ldap" Predefined Selected:
I Signature hature Name: hature: ocols:	jndi:ldap part="jndi:ldap" Predefined Selected: Thtp https
I Signature nature Name: nature: ocols:	jndi:ldap pat="indi:ldap" Predefined Image: Selected: Image: Predefined Predefined Selected: Image: Predefined Selected:
I Signature lature Name: lature: ocols: rch Signature In:	jndi:ldap patt="indi:ldap" Predefined Predefined Selected: http http http http tips Predefined Selected: Predefined Selected: Headers Vis And Parameters

→ Create butonu ile imza oluşturulur.

→ Son görüntü aşağıdaki gibi olmalıdır.

CVE-2021-44228 Log4J Vulnerability -	Manual, Web	+	*	CVE-2021-44228-r	egexp
Description:				Signature Name	CVE-2021-44228-regexp
 Q (X I < Page 1 of 1 ▶ ▶			Signature Pattern	part="\x24\x7b",rgxp="\x24\ {0,30}n.{0,30}d.{0,30}i.{0,30}
Name	Pattern	 Protocol 	-		Predefined
CVE-2021-44228-regexp	part="\x24\x7b",rgxp="\x24\x7b.{0,30}i.{0,30}n.{0,30}d.{0,30}i.{0,30}i.{1,150}"	http,https			
jndi:dns	part="jndi:dns"	http,https		Protocols:	
jndi:ldap	part="jndi:ldap"	http,https			
jndi:rmi	part="jndi:rmi"	http,https			
				Search Signature In:	Predefined Response Cor Urls And Parai

- 2. Custom Web Service politikası oluşturulması
- → Policies>Security sekmeleri takip edilir
- → + butonuna basılarak, seçenekler içinden web service seçilir.

	ERY & CLASSIFICATION SETUP	RISK MANAGEMEN	NT POLICIES A
Security Audit Data Enrichment S	ystem Events Action Sets		
Basic Filter Saved Filters	Policies		🛨 💢 Policy nam
By ADC Keywords	Policy	🚖 Туре	Web Service
Ву Туре	HTTP/1 x Protocol Validation		Web Application
By Level			DB Service
E By Server Group	Denemecusion sigpolicy	ni iF/i.	DB Application
By Service	DenemeCustom sigpolicy2	HTTP/1.	Network
By Application	HTTP/1.x Protocol Policy	HTTP/1.	Snippet Injection
Default Policies	Soliniection Plicy	HTTD/1	HDES Service
🔁 🕀 Policy Origin	Squiljeedon Filey	111 11 / 1.	7/OS DB Service
DB Protocol Validation			2/03 DD Service C
	SOL Protocol Policy	DB Proto	🖂 🗄 🖶 Sigr
	O QE FIOLOCOT FOILCY	DD FIOR	Available
	test	DB Proto	col

➔ Açılan sekmede ilgili zafiyetin ismi yazılır ve type olarak http protocol signitures seçilir.

	Create New Policy ×
ol S	Name CVE-2021-44228 Apache Log4j Vulnerability
ol S	From Scratch
ol S	Type: HTTP Protocol Signatures 🗸
01.5	OUse existing
	Access to Restricted Configuration Files
ol	
	Create Cancel
on	Signatures 1

Policy Rules sekmesinde + butonuna basarak 1. Aşamada oluşturmuş olduğumuz dictionary seçilir. Son durum ekran görüntüsünün aynısı olmalıdır. Yani Severity no alert ve action none olmalıdır.

	Policy name: CVE-2021-44228 Apache Log4j Vulnerability			Save
ſ	Policy Rules Apply To Advanced Activity Log			
ſ	Dictionary Name	Severity	Action	Followed Action
		Seventy	Action	1 ollowed Action
	CVE-2021-44228 Apache Log4j Vulnerability	No Alert 🗸	None 🗸	×

Değişiklikleri kayıt ettikten sonra, apply to sekmesinden ilgili servislere politika atanır.

Policy name: CVE-2021-44228 Apache Log4	4j Vulnerability
Policy Rules Apply To Advanced	Activity Log
É 🕞 🕞 All	
🕀 🚠 🗹 Apache	
Default Site	
🗈 📩 🗹 SuperVeda	
🖻 🚠 🔲 misc2012	

3. Web Servis custom politikası oluşturulması

→ Policies> Security sekmeleri takip edilir.

→ + butonuna basılarak, seçenekler içinden Web Service seçilir

SECURESPHERE DISCO	VERY & CLASSIFICATION SETUP RISK MANAGEMEN	NT POLICIES	AUDIT
Security Audit Data Enrichment	System Events Action Sets		
Basic Filter Saved Filters	Policies	🕂 🗯 Policy na	me: CVE-2
By ADC Keywords	14 4 Page 3 of 6 > >1	Web Service	riteria
By Type	Policy	Web Application	
By Server Group		DB Service	
	CVE-2018-20062: ThinkPHP 5 x Remote Code Execut	Network	Action:
By Application	CVE-2018-20062: ThinkPHP Permote Code Execution	Snippet Injection	e:
Default Policies Policy Origin	CVE-2018-20202: Anache Eineract Cleartext LIPL Cred	HDFS Service	Criteria
	CVE-2018-8823: PrestaShon Responsive Mera Menu	z/OS DB Service	le Match
<u><u><u></u></u></u>	CVE 2010-0023. Prestability Responsive wega went	note 🗄 🛧 Ad	- count Tak
	CVE 2019-10352 Git Client Plugin for Jenkins git Is-ten		oplication I

→ İlgili zafiyetin ismi oraya yazılır ve type olarak web service custom seçilir.

Create New Policy	ession	
Name CVE-2021-44228	B custom	
From Scratch Type:	Web Application Custom	~
OUse existing		
Anti Scrapin	g Policy	~
	Create Cance	
🗄 🛧 HTTP Request (Content-Type (Header)	
	Cookie Name	

→ Açılan panelde match criteria olarak signatures seçilir. Ve operations kısmında user defined signitures seçilir, daha sonrasında önceden oluşturmuş olduğumuz imzaları sol sekmeden, sağ(selected) sekmeye alınır. Oluşturmuş olduğumuz politikanın action'I block, severitysi high olmalıdır.

Match Criteria Apply To Advanced	
Policy Configuration: Signatures is at least one of [jndi:dns, jndi:r	m] Full Description
Action: Block Followed Action: gradar Alert Name: Custom Violation	Severity: High Enabled: One Alert Per Session: Interpret Alert Per Session: High High
Operation: At least one	v
User Defined Signatures	Selected: CVE-2021-44228-regexp jndi:ldap jndi:rmi
Available Match Criteria	
由 ★ Account Takeover Protection Results	
🗄 🛧 Application User	
Authenticated Session	
Client Type [ThreatPader Bet Protection]	

→ Apply to kısmında ilgili servisler seçilir.

Policy name: CVE-2021-44228 custom					
Match Criteria Apply To	Advanced	Activity Log			
ė- 📂 🖃 All					
🕒 📸 🗹 Apache					
🔤 🔂 🖂 Default Site					
🗈 🚠 🗹 SuperVeda					
🗄 🚠 📃 misc2012					

4. Monitor

Bu zafiyeti sömürmeye yönelik bir atak gelirse Monitor>Alerts kısmından CVE-2021-44228 politikasının tetiklendiğini görebilirsiniz.

SECURESPHERE DISCOVERY & CLASSIFICATION	N SETUP RISK MANAGEMENT POLICIES AUDIT REPORTS MONITOR THREATRADAR		
Dashboard Alerts Violations System Events Blocked	Sources Monitor System		
Quick Filter Alerts (filtered)	× (*	Alert 28024: CVE	-2021-44228 custom
	▶I	Antional	madiata Black
? Tips No O- II- U	odated - #- Alert Description	Policy:	VE-2021-44228 custom
Basic Filter Saved Filters	G _w	Edit Policy	Knowledge Base
E Last 2 Hours (2)	150-40 4 OVE 0004 44000 evolution		, and a go the o
By Immediate Action	1.32.42 4 <u>CVE-2021-44226 CUSION</u>	Aggregated fro	m 19:34:15 (0 hour(s), 1
By Alert Type	2 Multiple WEB-IIS cmd.exe access(+) from #+Ex+NHgUInm i D9tN i OuGyJM6pi9nWuPGGZ7XYUH0XA		
By Alert Flag		1 4	
By Alert Number			
By Server Group		0	
By Service			
By Application			
By User Name			
By Source IP		Alert aggregated	by:
By Protocol		Distinct value for	Value
By URL		Immediate Action	CVE-2021-44220 Block
By Session ID		Server Group	Apache Web SG
By Event ID		Source IP	192.168.95.25
By Remedy Incident ID			
By Gateway			
By Source GeoLocation			
Generated by ThreatRadar		Violations:	
By File Parent Path		Session	User URL
By Object Name			/twiki/twikidocu
By File Extension		I	/twiki/twikidocu
		III IN/A	/twiki/twikidocu
		III IN/A	/ WIN/ WINIUUCU

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-remotecode-execution-vulnerability